

**UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY**

**SENATOR DIANNE FEINSTEIN
CHAIR**

**SENATOR JON KYL
RANKING MEMBER**



**Seven Years after September 11:
Keeping America Safe**

110TH CONGRESS

**Report Submitted by Majority and Minority Staff
April 2009**

We calculated in advance the number of casualties from the enemy who would be killed based on the position of the [World Trade Center] tower. We calculated that the floors that would be hit would be three or four floors. I was the most optimistic of them all . . . due to my experience in this field, I was thinking that the fire from the gas in the plane would melt the iron structure of the building and collapse the area where the plane hit and all the floors above it only. This is all that we had hoped for.

— *Osama bin Laden*
November 2001¹

Since that terrible day, we have been spared another major attack on American soil. This is a significant achievement, made possible by the diligence of many courageous Americans defending us at home and overseas. But the threat that struck so terribly on 9/11 remains extremely dangerous. [Al Qaeda] and its affiliates have continued to strike at American and allied interests around the globe . . . These attacks are a reminder that the Al Qaeda network is an adaptable enemy, willing to exploit any complacency or oversights in our defenses. It is also a patient enemy: The attacks of 9/11, for example, were conceived by Khalid Sheik Mohammed in 1996. We can only assume that [Al Qaeda] and its affiliates continue to desire, and plan, further attacks against our homeland.

— *Thomas Kean and Lee Hamilton*
The 9/11 Public Discourse Project
September 2005²

¹ John Barry and Evan Thomas, *Evil in the Cross Hairs*, NEWSWEEK, Dec. 24, 2001, at 14 (transcript of the Osama bin Laden videotape).

² Thomas Kean and Lee Hamilton, *Reviewing Our Defenses, Four Years After 9/11*, FORWARD, Sept. 9, 2005, available at http://www.9-11pdp.org/press/2005-09-09_op-ed.pdf.

TABLE OF CONTENTS

OVERVIEW.....	2
EXECUTIVE SUMMARY	3
BORDER SECURITY.....	9
US-VISIT: Challenges and Strategies for Securing the U.S. Border	9
Introduction.....	9
US-VISIT: An Important Component in Securing the Border.....	9
System Requirements	10
Exit Procedures.....	11
Interim Solutions for Land Port Exit Procedures	12
The Need for Biometric Entry and Exit Systems in the Future.....	14
Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents.....	15
Introduction.....	15
The Urgency of Securing International Travel Documents.....	16
State Department Efforts to Combat Document Fraud.....	17
Forensic Documents Laboratory.....	19
Western Hemisphere Travel Initiative.....	19
Stolen and Lost Travel Document System	21
Potential Vulnerabilities: The Visa Waiver Program	23
Conclusion	24
Weaknesses in the Visa Waiver Program: Are the Needed Safeguards in Place to Protect America?	25
Introduction.....	25
VWP Vulnerabilities.....	27
Section 711 of the 9/11 Commission Act.....	29
Certifying the Air Exit Requirement: A Flawed Methodology	30
VWP Expansion.....	31
GAO Recommendations	32
Conclusion	33

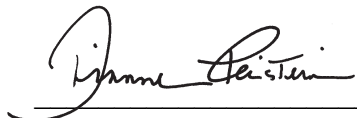
The Visa Waiver Program: Mitigating Risks to Ensure Safety of All Americans	34
Introduction.....	34
The Visa Waiver Program: Traditional Criticisms	35
Balancing Competing Interests.....	35
The 9/11 Commission Act.....	36
The Executive's Efforts to Expand the VWP	36
Subcommittee Action on the Planned Expansion of the VWP.....	36
GAO Findings.....	37
Certifying the 9/11 Act's Air Exit System Requirement.....	38
Electronic System for Travel Authorization (ESTA)	39
Overstays	41
Information Sharing.....	41
Lost or Stolen Passports.....	41
Concerns Regarding New Entrants and Visa Refusal Rates	42
Moving Forward	42
 DOMESTIC SECURITY	 43
 Identity Theft: Innovative Solutions for an Evolving Problem	 43
Introduction.....	43
Identity Theft: A Growing Problem	45
Causes of Identity Theft.....	45
Data Breaches	45
Data Breach Notification	46
The Federal Government's Efforts to Combat Identity Theft	47
President's Identity Theft Task Force.....	48
State Identity Theft Laws and Solutions.....	49
Notification of Risk to Personal Data Act (S. 239)	50
Conclusion	50
 The Legal Rights of Guantanamo Detainees: What Are They, Should They Be Changed, and Is an End in Sight?	 51
Introduction.....	51
Background.....	52
The History of Releasing Guantanamo Detainees	53
The Authority of Military Law During Wartime.....	54
Characteristics of the Military Commissions Act.....	55
Habeas Corpus Rights for Detainees	57
Characteristics of the Detainee Treatment Act.....	58
No Precedent for Extending Habeas Corpus Rights to Detainees	58

Negative Effects of Habeas-Type Litigation on Interrogation of Detainees	59
Characteristics of the Detainee Treatment Act.....	60
Conclusion	61
Appendix: Hearings During the 110th Congress.....	62
US-VISIT: Challenges and Strategies for Securing the U.S. Border	62
Identity Theft: Innovative Solutions for an Evolving Problem	63
Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents	64
The Legal Rights of Guantanamo Detainees: What Are They, Should They Be Changed, and Is an End in Sight?	65
Weaknesses in the Visa Waiver Program: Are the Needed Safeguards in Place to Protect America?.....	66
The Visa Waiver Program: Mitigating Risks to Ensure Safety of All Americans	67

INTRODUCTION

On the morning of September 11, 2001, the nation and the world changed forever when 19 terrorists hijacked four commercial planes: American Airlines Flight 11 crashed into the North Tower of the World Trade Center; United Airlines Flight 175 crashed into the South Tower of the World Trade Center; American Airlines Flight 77 crashed into the Pentagon; and United Airlines Flight 93 crashed in Somerset County, Pennsylvania.³ Masterminded by Osama bin Laden and his Al Qaeda terrorist network, the attacks killed 3,016 people and wounded thousands more.⁴

Seven years after September 11, the Subcommittee on Terrorism, Technology, and Homeland Security focused its efforts during the 110th Congress on securing our borders, protecting personally identifiable information, and resolving legal issues related to the war against terrorists. To this end, the Subcommittee held hearings on vulnerabilities in international travel processes, the evolving problems of identity theft, and the establishment of a system of trial and detention that balances the rights of enemy detainees with the need to protect our nation from future attacks. The attached report is a summary of the Subcommittee's efforts to understand these issues and determine what remains to be done to secure the homeland.



DIANNE FEINSTEIN

Chair

Subcommittee on Terrorism,
Technology, and Homeland Security
Committee on the Judiciary
United States Senate



JON KYL

Ranking Member

Subcommittee on Terrorism,
Technology, and Homeland Security
Committee on the Judiciary
United States Senate

³ *A Nation Challenged: Indictment Chronicles "Overt Acts" That It Says Led to Sept. 11 Attacks*, N.Y. TIMES, Dec. 12, 2001, at B6.

⁴ James Barron, *Two Years Later: Ceremonies; Another 9/11, and a Nation Mourns Again*, N.Y. TIMES, Sept. 12, 2003, at A1; David Chen, *Man Behind Sept. 11 Fund Describes Effort as a Success, With Reservations*, N.Y. TIMES, Jan. 1, 2004, at B1.

Seven Years After September 11: Keeping America Safe

OVERVIEW

In the 110th Congress, the Subcommittee on Terrorism, Technology, and Homeland Security was one of the Senate Judiciary Committee's most active Subcommittees. The Subcommittee investigated the Department of Homeland Security's progress in implementing the US-VISIT entry and exit system at U.S. ports of entry, the need to secure international travel documents, vulnerabilities in the Visa Waiver Program, the federal government's efforts to combat identity theft, and the legal rights of enemy combatants. The Subcommittee's efforts in these areas were successful, leading to the introduction of legislation that would strengthen international travel documents and the Visa Waiver Program,¹ and to the advancement of legislation that would help provide notice to the American people when their personal information has been compromised.²

The Subcommittee's efforts to promote effective governance require vigorous and effective oversight of the departments within its jurisdiction. Most important, of course, are the Departments of Justice and Homeland Security. The Subcommittee directs significant resources to this end, and welcomes the submission of briefings or reports that supplement its own independent research. These resources complement the hearing process and serve as mechanisms for further understanding the successes and failures of policies designed to secure the border and combat terrorism. Although issues within the Subcommittee's jurisdiction are among the most sensitive in America, the Subcommittee has crafted a bipartisan approach to oversight, as illustrated by this joint report.

¹ Strengthening the Visa Waiver Program to Secure America Act, S. 203, 111th Cong. (2009).

² Notification of Risk to Personal Data Act of 2007, 110th Cong. (2007); Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, 110th Cong. (2007).

EXECUTIVE SUMMARY

Key findings and accomplishments:

Border Security

The Department of Homeland Security (DHS) has made substantial gains in implementing US-VISIT entry procedures, but has not yet implemented the statutorily required US-VISIT exit procedures. In its efforts to secure our nation's borders, the Subcommittee convened a hearing to highlight the government's inability to determine reliably who is exiting the United States.³ Senators Feinstein and Kyl were particularly concerned about the federal government's failure to fully implement the United States Visitor and Immigrant Status Indicator Technology (US-VISIT), an automated system that utilizes biometric information to document the entry and exit of travelers at all U.S. ports. Senator Feinstein emphasized that by failing to produce an effective exit system at all ports of entry, "we are providing a blueprint to those who wish to harm the United States."⁴ Senators Feinstein and Kyl remain concerned about the lack of an effective exit component, and will work with the Department in future Congresses to ensure that law enforcement and intelligence officials can track who is entering and exiting our nation.

The use of fraudulent international travel documents poses a serious threat to the national security of the United States. Recognizing that fraudulent documents might facilitate terrorist travel, the Subcommittee held a hearing to investigate the federal government's initiatives to: (1) identify persons traveling with fraudulent documents; (2) make travel documents more secure; and (3) improve traveler screening at ports of entry.⁵ According to Andrew Simkin's testimony, the State Department is using advanced

³ *US-VISIT: Challenges and Strategies for Securing the U.S. Border: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 1st Sess. (Jan. 31, 2007) (S. Hrg. 110-20, Serial No. J-110-6), at 1 (statement of Dianne Feinstein) [hereinafter "Hearing of Jan. 31, 2007"].

⁴ Hearing of Jan. 31, 2007, at 2 (statement of Dianne Feinstein).

⁵ *Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 1st Sess. (May 2, 2007) (S. Hrg. 110-103, Serial No. J-110-32), at 3 (statement of Dianne Feinstein) [hereinafter "Hearing of May 2, 2007"].

technologies to check biometric data against terrorist watchlists and has introduced a new, more secure passport.⁶ Mr. Simkin also suggested that the Department is deploying additional personnel to “critical” posts overseas to investigate and disrupt passport and visa fraud.⁷ According to Michael Everitt, other efforts also are underway to address this issue. For instance, the Department of Homeland Security’s Forensic Documents Laboratory is working to detect and deter the use of fraudulent documents, providing real-time support and training to law enforcement personnel worldwide,⁸ and developing higher-quality and more secure documents.⁹ Additionally, DHS is working with the State Department to implement the Western Hemisphere Travel Initiative,¹⁰ and is working with Interpol to implement the Stolen and Lost Travel Documents (SLTD) system, an international database that currently includes data on stolen and lost passports from 123 countries.¹¹ Despite these efforts, however, gaps in the document-security system remain. The Visa Waiver Program permits 15 million travelers to enter the United States each year after only minimal screening,¹² and of the 6.7 million passports registered in the SLTD database, 2.7 million are from visa waiver countries.¹³ In an effort to address existing security gaps, Senators Feinstein, Kyl, and Sessions introduced legislation that would bolster penalties for passport fraud offenses.¹⁴

The Visa Waiver Program (VWP) is likely expanding too quickly given its lack of required safety features and continued security risks. The VWP is a reciprocal agreement between the United States and 27 other countries meant to facilitate trade, travel, and international goodwill by allowing foreign nationals to enter the United States without a visa for up to 90 days.¹⁵ According to the Government Accountability Office, however, the program

⁶ Hearing of May 2, 2007, at 6 (statement of Andrew Simkin).

⁷ Hearing of May 2, 2007, at 7-8 (statement of Patrick Donovan).

⁸ Hearing of May 2, 2007, at 9-12 (statement of Michael Everitt).

⁹ Hearing of May 2, 2007, at 9 (statement of Michael Everitt).

¹⁰ Hearing of May 2, 2007, at 13 (statement of Paul Morris).

¹¹ Hearing of May 2, 2007, at 30 (statement of Ronald K. Noble).

¹² Hearing of May 2, 2007, at 13 (statement of Paul Morris).

¹³ Hearing of May 2, 2007, at 30 (statement of Ronald K. Noble).

¹⁴ Passport and Visa Security Act of 2007, S. 276, 110th Cong. (2007).

¹⁵ GAO, *Visa Waiver Program: Limitations with Department of Homeland Security’s Plan to Verify Departure of Foreign Nationals*, GAO-08-458T, at 1 (Washington, D.C., Feb. 28, 2008).

could also be exploited by terrorists, criminals, or those seeking to violate our immigration laws.¹⁶ Concerned about the VWP's vulnerabilities, the Subcommittee held a hearing to determine whether the Department of Homeland Security's proposed expansion of the VWP in accordance with the provisions of the 9/11 Act¹⁷ was appropriate. Testimony provided by Jess Ford, the Government Accountability Office's witness, suggested that DHS's expansion plans were likely not compliant with the 9/11 Act's requirements,¹⁸ and Senators Feinstein, Kyl, and Sessions agreed.¹⁹ The Subcommittee's efforts led to a second hearing concerning the VWP in the 110th Congress and the introduction of legislation by Senators Feinstein and Kyl in the 111th Congress.²⁰

The Visa Waiver Program's planned expansion to include countries requiring waivers of traditional safety metrics continues to pose immigration and national security risks. Concerned by its findings at the hearing on February 28, 2008 and subsequent communications with the Secretary of the Department of Homeland Security, the Subcommittee convened a second hearing to investigate the Visa Waiver Program (VWP) on September 24, 2008.²¹ Of particular concern was a GAO report, issued September 15, 2008,²² which reiterated GAO's concerns and those previously raised by Senators Feinstein and Kyl about the Executive's planned expansion of the VWP and its compliance with relevant provisions of the "Implementing Recommendations of the 9/11 Commission Act of 2007" (the 9/11 Act).²³

¹⁶ GAO, *Visa Waiver Program: Limitations with Department of Homeland Security's Plan to Verify Departure of Foreign Nationals*, GAO-08-458T, at 1 (Washington, D.C., Feb. 28, 2008).

¹⁷ GAO, *Visa Waiver Program: Actions Are Needed to Improve Management of the Expansion Process, and to Assess and Mitigate Program Risks*, GAO-08-967, at 2 (Washington, D.C., Sept. 15, 2008) [hereinafter "GAO Rep. of Sept. 15, 2008"].

¹⁸ *Weaknesses in the Visa Waiver Program: Are the Needed Safeguards in Place to Protect America?: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 2d Sess. (Feb. 28, 2008) (S. Hrg. 110-473, Serial No. J-110-77), at 9 (statement of Jess Ford) [hereinafter "Hearing of Feb. 28, 2008"].

¹⁹ Hearing of Feb. 28, 2008, at 23 (statement of Jon Kyl).

²⁰ Strengthening the Visa Waiver Program to Secure America Act, S. 203, 111th Cong. (2009).

²¹ *The Visa Waiver Program: Mitigating Risks to Ensure Safety of All Americans: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 2d Sess. (Sept. 24, 2008) (S. Hrg. 110-674, Serial No. J-110-121), at 1 (statement of Dianne Feinstein).

²² GAO Rep. of Sept. 15, 2008.

²³ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 338 (2007).

Despite the concerns expressed by the Senators Feinstein and Kyl and the GAO, the administration moved forward with its planned expansion of the Visa Waiver Program using its authority under the 9/11 Act.²⁴ That expansion led Senators Feinstein and Kyl to introduce legislation that would address many of the concerns raised about the VWP at the Subcommittee's hearings during the 110th Congress.²⁵

Domestic Security

Identity theft is a nationwide problem that costs consumers and businesses \$50 billion and affects more than 8.4 million consumers each year.²⁶ In the past nine years, the Subcommittee has held eight hearings on identity theft in an effort to ensure the security and financial privacy of U.S. citizens and businesses.²⁷ During the 110th Congress, the Subcommittee

²⁴ Department of Homeland Security, *DHS Reminds Visa Waiver Program Travelers of ESTA Requirements Effective Today*, http://www.dhs.gov/xnews/releases/pr_1231771555521.shtm (last visited Mar. 5, 2009).

²⁵ Strengthening the Visa Waiver Program to Secure America Act, S. 203, 111th Cong. (2009).

²⁶ *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 1st Sess. (Mar. 21, 2007) (S. Hrg. 110-62, Serial No. J-110-22), at 3 (statement of Jon Kyl) [hereinafter "Hearing of Mar. 21, 2007"].

²⁷ *Database Security: Finding Out When Your Information Has Been Compromised: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108th Cong., 1st Sess. (Nov. 4, 2003) (S. Hrg. 108-520, Serial No. J-108-52); *Identity Theft Penalty Enhancement Act of 2002: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 2nd Sess. (July 9, 2002) (S. Hrg. 107-900, Serial No. J-107-68); *Identity Theft: Restoring Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 2nd Sess. (Mar. 20, 2002) (S. Hrg. 107-900, Serial No. J-107-68); *Privacy, Identity Theft, and the Protection of your Personal Information in the 21st Century: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 2nd Sess. (Feb. 14, 2002) (S. Hrg. 107-852, Serial No. J-107-60); *Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 1st Sess. (Nov. 14, 2001) (S. Hrg. 107-657, Serial No. J-107-46A); *Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106th Cong., 2nd Sess. (July 12, 2000) (S. Hrg. 106-902, Serial No. J-106-97); *ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106th Cong., 2nd Sess. (Mar. 7, 2000) (S. Hrg. 106-885, Serial No. J-106-70); *The Identity Theft and Assumption Deterrence Act: S. 512: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 105th Cong., 2nd Sess. (May 20, 1998) (S. Hrg. 105-845, Serial No. J-105-104).

continued its focus on securing personally identifiable information, investigating the federal government's role in preventing criminals from illegally or improperly obtaining and misusing sensitive, personally identifiable information.²⁸ For instance, at the time of the hearing, the Department of Justice and the Federal Trade Commission were actively prosecuting identity theft cases and educating consumers and businesses about identity theft.²⁹ President Bush had also established the President's Identity Theft Task Force in May 2006 "to use Federal resources effectively to deter, prevent, detect, investigate, proceed against, and prosecute" identity theft.³⁰ Building upon these efforts, Senators Feinstein and Kyl supported legislation to address the issue of data breaches, a form of large-scale identity theft that can harm individuals, create economic losses, and stifle commerce.³¹ In 2005 and 2006, over 100 million data records containing sensitive consumer data were compromised due to data breaches.³² In January 2007, Senator Feinstein introduced S. 239, the Notification of Risk to Personal Data Act,³³ which would create a federal data breach notification law, and Senator Kyl cosponsored similar legislation, S. 2102, the Personal Data Protection Act.³⁴

The federal government must devise a system of trial and detention for alien enemy combatants in the war against terrorists that can withstand constitutional scrutiny while protecting the American people from further attack. The asymmetric nature of the war against terrorists has raised new questions about the legal rights of alien enemy combatants, particularly those detained at the detention facility at Guantanamo Bay. For instance, the federal government must decide who has the authority to determine a detainee's legal

²⁸ President's Identity Theft Task Force, *Interim Recommendations* 1 (Sept. 2006), available at <http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf>; hearing of Mar. 21, 2007, at 2-3 (written statement of Lydia Parnes).

²⁹ Hearing of Mar. 21, 2007, at 1 (written statement of Ronald Tenpas); *id.* at 7-8 (statement of Lydia Parnes).

³⁰ Strengthening Federal Efforts to Protect Against Identity Theft, Exec. Order No. 13,402, 71 C.F.R. 27,945 (May 10, 2006), available at <http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html>.

³¹ Hearing of Mar. 21, 2007, at 1-2 (statement of Dianne Feinstein).

³² Hearing of Mar. 21, 2007, at 2 (statement of Dianne Feinstein).

³³ Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. §§ 2-3, 7 (2007).

³⁴ Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007).

status — the military or the federal judiciary.³⁵ The Subcommittee convened a hearing to investigate these and other issues related to the legal rights of alien enemy combatants. While the Subcommittee's members expressed a variety of opinions at the hearing, they generally agree that Congress can and should establish a system of trial and detention that is fair for the detainees, but recognize the need to protect the safety and security of Americans.

³⁵ *The Legal Rights of Guantanamo Detainees: What Are They, Should They Be Changed, and Is an End in Sight?: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 1st Sess. (Dec. 11, 2007) (S. Hrg. 110-____, Serial No. J-110-____), at 64 (transcript) (statement of Lindsey Graham) [hereinafter "Hearing of Dec. 11, 2007"].

BORDER SECURITY

US-VISIT: Challenges and Strategies for Securing the U.S. Border

Introduction

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is an automated system that will utilize biometric information to document the entry and exit of travelers at all U.S. ports. This system is designed to protect the security of U.S. citizens and visitors, facilitate trade and commerce, guard U.S. visitor privacy, and enforce immigration law.³⁶

On January 31, 2007, the Subcommittee held a hearing entitled “US-VISIT: Challenges and Strategies for Securing the U.S. Border.” The hearing was convened to investigate the Department of Homeland Security’s (DHS) progress in implementing the US-VISIT entry and exit systems at U.S. ports of entry. Two panels provided testimony at the hearing. Panel one consisted of (1) Richard Barth, Assistant Secretary, Office of Policy Development, DHS; and (2) Robert Mocny, acting Director, US-VISIT Program, DHS. Panel two consisted of (1) Richard Stana, Director, Homeland Security and Justice Issues, the Government Accountability Office (GAO); (2) Phillip Bond, President and Chief Executive Officer, Information Technology Association of America; and (3) Stewart Verdery, Partner and Founder, Monument Policy Group.

US-VISIT: An Important Component in Securing the Border

At the outset of the hearing, Senator Feinstein noted that “the Federal Government has failed to devote sufficient time, technology, personnel and resources to making border security a cornerstone of our national security policy.”³⁷ Of particular concern is the government’s inability to determine reliably who is exiting the United States: without knowing who is leaving the country, it cannot be determined who is overstaying his or her visa.³⁸ Although the US-VISIT entry system has been

³⁶ *US-VISIT: Challenges and Strategies for Securing the U.S. Border: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 1st Sess. (Jan. 31, 2007) (S. Hrg. 110-20, Serial No. J-110-6), at 18 (statement of Robert Mocny) [hereinafter “Hearing of Jan. 31, 2007”].

³⁷ Hearing of Jan. 31, 2007, at 1 (statement of Dianne Feinstein).

³⁸ Hearing of Jan. 31, 2007, at 2 (statement of Dianne Feinstein).

implemented with some success at all types of ports, the exit component of US-VISIT has yet to be implemented at any type of port.³⁹

Mr. Mocny testified that the progress DHS has made with US-VISIT has improved immigration and border security.⁴⁰ Since January 2004, DHS has “intercepted approximately 1,800 immigration violators and people with criminal histories,”⁴¹ and “Immigration and Customs Enforcement officials have made more than 290 arrests based on US-VISIT overstay information.”⁴²

System Requirements

The hearing discussed what must be considered beyond the statutory requirements to render US-VISIT effective. First, US-VISIT must be integrated with other security and border systems.⁴³ Senator Cornyn noted that even if the exit programs were operational, it would make little impact if immigration laws could not be enforced against aliens who overstay their visas.⁴⁴

Mr. Mocny commented that, in an effort to encourage that integration, DHS was conducting a pilot program to provide federal, state, and local law enforcement with biometric and criminal information collected when foreign visitors enter the country.⁴⁵ DHS is also improving the fingerprint collection system used for non-citizen travelers. Whereas the old system required only two-fingerprint collection, the new system will be based on ten-fingerprint collection methodology, which will offer greater interoperability among border security and law enforcement agencies.⁴⁶

Second, US-VISIT must account for traffic and trade. Senator Cornyn stated that the impact to travel and trade needs to be weighed heavily:⁴⁷ “No enforcement system . . . should be adopted without assessing the impact it will have on legitimate

³⁹ Hearing of Jan. 31, 2007, at 2 (statement of Dianne Feinstein).

⁴⁰ Hearing of Jan. 31, 2007, at 7-8 (statement of Robert Mocny).

⁴¹ Hearing of Jan. 31, 2007, at 7 (statement of Robert Mocny).

⁴² Hearing of Jan. 31, 2007, at 8 (statement of Robert Mocny).

⁴³ Hearing of Jan. 31, 2007, at 17 (statement of Richard Stana).

⁴⁴ Hearing of Jan. 31, 2007, at 12 (statement of John Cornyn).

⁴⁵ Hearing of Jan. 31, 2007, at 8 (statement of Robert Mocny).

⁴⁶ Hearing of Jan. 31, 2007, at 8 (statement of Robert Mocny); *id.* at 5 (statement of Richard Barth).

⁴⁷ Hearing of Jan. 31, 2007, at 3 (statement of John Cornyn).

travel and trade to the United States. Our Nation's security is paramount, to be sure, but trade, especially with our partners on the Northern and Southern borders, is critical to the health of our economy.”⁴⁸

Finally, it was noted that US-VISIT is not a substitute for customs officials who visually inspect the traveler. Mr. Stana explained, “keep in mind that Ahmed Ressam, the Millennium Bomber, was stopped not by technology but by an alert customs inspector who observed the subject and had a gut instinct that something was not quite right.”⁴⁹

Exit Procedures

Implementation of the US-VISIT exit component has proven problematic since no existing port was designed to accommodate exit control: “an exit solution presents not only an infrastructure challenge, but, equally important, a fundamental change in the business process of travelers who are departing the United States.”⁵⁰

DHS has begun implementation of the exit component at airports. Priority was placed on airports because 91 percent of those travelers subject to US-VISIT review arrive in the United States via airplane.⁵¹ Airports are the easiest type of port to deploy US-VISIT because much of the needed infrastructure is already available,⁵² and there is a lesser chance of delaying traffic or trade.⁵³

Mr. Verdery testified that, to prevent further delay in the implementation of US-VISIT at airports, DHS needs to end deliberation and choose how to deploy the system.⁵⁴ He explained that there is still uncertainty about where passengers should undergo exit screening — at the check-in counter or the boarding gate.⁵⁵ To enforce the airport US-VISIT exit system in airports, the United States could require that all those who enter via air under the Visa Waiver Program be required to exit via air, or else be

⁴⁸ Hearing of Jan. 31, 2007, at 3 (statement of John Cornyn).

⁴⁹ Hearing of Jan. 31, 2007, at 17 (statement of Richard Stana).

⁵⁰ Hearing of Jan. 31, 2007, at 6 (statement of Richard Barth).

⁵¹ Hearing of Jan. 31, 2007, at 6 (statement of Richard Barth).

⁵² Hearing of Jan. 31, 2007, at 20 (statement of Stewart Verdery).

⁵³ Hearing of Jan. 31, 2007, at 5-6 (statement of Richard Barth).

⁵⁴ Hearing of Jan. 31, 2007, at 20 (statement of Stewart Verdery).

⁵⁵ Hearing of Jan. 31, 2007, at 20 (statement of Stewart Verdery).

registered as an overstayer.⁵⁶ Also, the security requirements for the airport exit system could be an admission criterion for the nations that seek to join the Visa Waiver Program; this criterion would provide an incentive for other countries to meet these requirements.⁵⁷

With current technology, the only way to implement a biometric exit system for land ports would be to create a “mirror image” of the entry system.⁵⁸ DHS does not believe that such duplication is a viable option because the costs would be “astronomical.”⁵⁹ A mirror image would require major infrastructure improvements, land acquisitions, and additional staffing. It would also create longer wait times for travelers and commerce.⁶⁰ Current technology is inadequate to tackle these problems, but DHS is closely monitoring technological advances.⁶¹ In the meantime, DHS is looking to interim solutions.⁶²

Interim Solutions for Land Port Exit Procedures

After deploying the exit procedures for the air and sea ports, DHS will concentrate on land ports.⁶³ Exit procedures for land ports are the most complicated and costly to implement and operate.⁶⁴

Radio frequency identification (RFID)⁶⁵ is one interim solution that has been tested at various land ports. Mr. Mocny said that RFID is a viable solution in the

⁵⁶ Hearing of Jan. 31, 2007, at 23 (statement of Stewart Verdery).

⁵⁷ Hearing of Jan. 31, 2007, at 21 (statement of Stewart Verdery).

⁵⁸ Hearing of Jan. 31, 2007, at 10 (statement of Richard Barth).

⁵⁹ Hearing of Jan. 31, 2007, at 10 (statement of Richard Barth).

⁶⁰ Hearing of Jan. 31, 2007, at 6 (statement of Richard Barth).

⁶¹ Hearing of Jan. 31, 2007, at 6 (statement of Richard Barth).

⁶² Hearing of Jan. 31, 2007, at 6 (statement of Richard Barth).

⁶³ Hearing of Jan. 31, 2007, at 6 (statement of Richard Barth).

⁶⁴ Hearing of Jan. 31, 2007, at 6 (statement of Richard Barth).

⁶⁵ RFID Journal, *What is RFID?*, <http://www.rfidjournal.com/faq/16/49> (last visited Feb. 20, 2009) (RFID is “a generic term for technologies that use radio waves to automatically identify people or objects. There are several methods of identification, but the most common is to store a serial number that identifies a person or object, and perhaps other information, on a microchip that is attached to an antenna (the chip and the antenna together are called an RFID transponder or an RFID tag). The antenna enables the chip to transmit the identification information to a reader. The reader converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers that can make use of it.”).

interim, but he admitted that RFID has many problems that need to be resolved.⁶⁶ Mr. Stana disagreed that RFID is a viable solution, explaining that “[RFID] had a success rate of only fourteen percent in one test and provided no assurance that the person recorded as leaving the country is the same one who entered.”⁶⁷ No exit procedures other than RFID have been tested at land ports, and RFID testing has currently been discontinued.⁶⁸

Mr. Bond, on the other hand, argued that with some improvements to RFID technology, it could function more accurately and at a comparably lower cost than other interim solutions.⁶⁹ For example, RFID could be attached to an I-94, which is a paper document used to record the entry and exit of foreign visitors.⁷⁰ Though the RFID/I-94 still would not meet the biometric requirement of ensuring that the card is being held by the person it belongs to, random testing could be used to deter fraudulent use of the document.⁷¹ Mr. Verdery agreed that the RFID/I-94 system could be adapted to work in the interim, but a biometric system is still the ultimate solution.⁷²

Regarding possible interim solutions in general, Mr. Stana cautioned “against taking a step that would lead the U.S. to a large investment that would not ultimately be the solution we are looking for.”⁷³ Additionally, Senator Cornyn warned of being lulled into “a false sense of security” regarding border security.⁷⁴ Senator Feinstein stated that “we have to walk before we run, . . . we should work on [a system], even if it is a paper system . . . to try to bring about a continuum of order and have it cost-effective.”⁷⁵ To develop more ideas, DHS is reviewing the departure control systems of other nations in its search for a permanent solution.⁷⁶ This process may be of little help because the

⁶⁶ Hearing of Jan. 31, 2007, at 8 (statement of Robert Mocny).

⁶⁷ Hearing of Jan. 31, 2007, at 16 (statement of Richard Stana).

⁶⁸ Hearing of Jan. 31, 2007, at 9 (statement of Robert Mocny).

⁶⁹ Hearing of Jan. 31, 2007, at 18-19, 22-23 (statement of Phillip Bond).

⁷⁰ Hearing of Jan. 31, 2007, at 18-19, 22-23 (statement of Phillip Bond).

⁷¹ Hearing of Jan. 31, 2007, at 21-22 (statement of Phillip Bond).

⁷² Hearing of Jan. 31, 2007, at 27 (statement of Stewart Verdery).

⁷³ Hearing of Jan. 31, 2007, at 24 (statement of Richard Stana).

⁷⁴ Hearing of Jan. 31, 2007, at 28 (statement of John Cornyn).

⁷⁵ Hearing of Jan. 31, 2007, at 24 (statement of Dianne Feinstein).

⁷⁶ Hearing of Jan. 31, 2007, at 14 (statement of Robert Mocny).

nations of interest have had the exiting infrastructures in place, and the United States has not.⁷⁷

The Need for Biometric Entry and Exit Systems in the Future

The Subcommittee supports the Department of Homeland Security's efforts to bolster our nation's security through US-VISIT, but Senators Feinstein and Kyl believe that greater emphasis should be placed on establishing effective biometric entry and exit systems. In particular, Senator Feinstein expressed disappointment with DHS for its failure to submit to Congress a statutorily required report that was due in June 2005. This report would have described the status of the biometric system in use and the progress of meeting the statutory goal of a biometric screening system for entry and exit.⁷⁸ Mr. Barth stated that DHS would send the Senate the strategies for the 2007 budget, which would provide a report detailing the kinds of testing and systems being pursued.⁷⁹

On December 18, 2008, DHS announced that it was "expanding the categories of non-U.S. citizens required to provide digital fingerprints and a photograph upon entry to the United States through the US-VISIT program"⁸⁰ and that US-VISIT had "deployed 10-print scanner technology to almost 80 percent of lanes at airports, seaports and secondary inspection areas of land ports of entry."⁸¹ DHS emphasized that the "[c]ollection and verification of biometric identifiers upon entry protects travelers by making it virtually impossible for anyone else to attempt to use their biometrically

⁷⁷ Hearing of Jan. 31, 2007, at 14 (statement of Robert Mocny).

⁷⁸ Hearing of Jan. 31, 2007, at 2 (statement of Dianne Feinstein).

⁷⁹ Hearing of Jan. 31, 2007, at 10 (statement of Richard Barth); in May 2007, DHS submitted to the requisite committees of jurisdiction, including the Senate Judiciary Committee, a report which fulfills the requirements of Section 7208(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458, IRTPA). This report discusses current technological capabilities for the screening of persons within our immigration and border management system; discusses areas of deficiency in both technology and process; and provides an end-vision on how the Department can build synergies between functional areas to optimize the security of our Nation's borders.

⁸⁰ Department of Homeland Security, *Department of Homeland Security Expands Collection of Biometrics for Visitors*, http://www.dhs.gov/xnews/releases/pr_1229620172131.shtm (last visited Feb. 24, 2009).

⁸¹ Department of Homeland Security, *Fact Sheet: DHS End-of-Year Accomplishments*, http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm (last visited Feb. 25, 2009).

linked travel documents (such as a permanent resident card) . . . if their documents were stolen or duplicated.”⁸²

DHS is also working to make its “Automated Biometric Identification System (IDENT) database interoperable with the FBI’s Integrated Automated Fingerprint Identification System (IAFIS).”⁸³ According to DHS, “IDENT/IAFIS interoperability will increase DHS and the State Department’s ability to screen travelers, increase accuracy of matching and provide greater ability to match against latent fingerprints — full or partial fingerprint ‘images’ left at the scene of a crime.”⁸⁴ DHS believes that “[t]he integration process now under way will benefit the FBI and other law enforcement organizations by providing them with increased access, during the interim solution, to information on high-risk persons refused visas and those removed from the United States.”⁸⁵

Though these are all important steps, Senators Feinstein and Kyl remain concerned about the exit component of US-VISIT, and will work with DHS in future Congresses to ensure that law enforcement and intelligence officials can account for who is entering and exiting our borders.

Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents

Introduction

On May 2, 2007, the Subcommittee on Terrorism, Technology, and Homeland Security held a hearing entitled “Interrupting Terrorist Travel: Strengthening the

⁸² Department of Homeland Security, *Department of Homeland Security Expands Collection of Biometrics for Visitors*, http://www.dhs.gov/xnews/releases/pr_1229620172131.shtm (last visited Feb. 24, 2009).

⁸³ Email from Ted Lovett, Associate Director, Office of Legislative Affairs, Department of Homeland Security, to Tom Humphrey, Legislative Aide, Senate Judiciary Committee (Mar. 3, 2009, 09:49:00 EST) (on file with author or recipient).

⁸⁴ Email from Ted Lovett, Associate Director, Office of Legislative Affairs, Department of Homeland Security, to Tom Humphrey, Legislative Aide, Senate Judiciary Committee (Mar. 3, 2009, 09:49:00 EST) (on file with author or recipient).

⁸⁵ Email from Ted Lovett, Associate Director, Office of Legislative Affairs, Department of Homeland Security, to Tom Humphrey, Legislative Aide, Senate Judiciary Committee (Mar. 3, 2009, 09:49:00 EST) (on file with author or recipient).

Security of International Travel Documents” to inquire whether federal agencies are taking advantage of all the tools at their disposal to identify travelers seeking to enter the United States with “bad motives.”⁸⁶

Seven experts testified at the hearing: (1) Andrew Simkin, Director, Office of Fraud Prevention Programs, Bureau of Consular Affairs, Department of State; (2) Patrick D. Donovan, Assistant Director for Diplomatic Security, Director of Domestic Operations, Bureau of Diplomatic Security, Department of State; (3) Michael Everitt, Unit Chief, Forensic Documents Laboratory, Immigration and Customs Enforcement, Department of Homeland Security (DHS); (4) Paul Morris, Executive Director, Admissibility Requirements and Migration Control, Office of Field Operations, Customs and Border Protection, DHS; (5) Ronald K. Noble, Secretary General, Interpol; (6) Clark Kent Ervin, Director of Homeland Security, Aspen Institute, and former Inspector General, DHS; and (7) Brian Zimmer, Senior Associate, Kelly, Anderson, and Associates, and former Senior Investigator, Committee on the Judiciary, House of Representatives.

The Urgency of Securing International Travel Documents

International travel documents, Senator Feinstein noted, are “as important as weapons” to terrorists,⁸⁷ as forged passports can permit terrorists to gain entry to, or establish citizenship in, countries throughout the world.⁸⁸ Interpol reports more than 14 million stolen or lost travel documents from 123 countries,⁸⁹ and since the 9/11 attacks, 24 of the 353 individuals classified as terrorists by the Department of Justice have been charged with document crimes.⁹⁰ Two of the 9/11 hijackers used altered passports to enter the United States, and as many as five of the 19 had some irregularity in their documents.⁹¹

⁸⁶ *Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary, 110th Cong., 1st Sess. (May 2, 2007) (S. Hrg. 110-103, Serial No. J-110-32), at 1 (statement of Dianne Feinstein).*

⁸⁷ Hearing of May 2, 2007, at 1 (statement of Dianne Feinstein).

⁸⁸ Hearing of May 2, 2007, at 3 (statement of Dianne Feinstein).

⁸⁹ Hearing of May 2, 2007, at 30 (statement of Ronald K. Noble).

⁹⁰ Hearing of May 2, 2007, at 2 (statement of Dianne Feinstein).

⁹¹ Hearing of May 2, 2007, at 2 (statement of Dianne Feinstein).

Although fraudulent documents may facilitate terrorists' travel, international travel also requires terrorists to "surface to pass through regulated channels" as they travel across borders, and thus provides key opportunities for law enforcement to interrupt terrorists' plans, including when they apply for visas, check in at an airport, or undergo port-of-entry screening.⁹² According to findings from 2004, DHS customs inspectors still admitted travelers using stolen passports 73 percent of the time, even when the inspectors knew the documents were stolen.⁹³ Customs officers also often return stolen passports to their carriers, allowing the carrier to use the fraudulent document in the future.⁹⁴ Unfortunately, "[d]ue to the limited data collected by inspectors at ports of entry, [DHS was] often unable to determine the inspector's rationale for having admitted the aliens."⁹⁵ Given the prevalence of document fraud and the critical importance of reducing it, cooperation between the Department of State, DHS, and Interpol is essential "to ensure that the front-line inspectors, those at airports and consular offices, have real-time access to lost and stolen passport databases," and to guaranteeing that inspectors are properly trained to use such databases effectively.⁹⁶

State Department Efforts to Combat Document Fraud

At the center of the State Department's efforts to combat document fraud are new technologies and bolstered human resources. According to Mr. Simkin, improved interagency data-sharing is allowing biographic and biometric information to be

⁹² Hearing of May 2, 2007, at 5 (statement of Andrew Simkin).

⁹³ Hearing of May 2, 2007, at 27 (statement of Clark Kent Ervin).

⁹⁴ Hearing of May 2, 2007, at 27 (statement of Clark Kent Ervin).

⁹⁵ *October 2005 Statutory Deadline for Visa Waiver Program Countries to Produce Secure Passports: Why it Matters to Homeland Security: Hearing Before the Subcomm. on Immigration, Border Security, and Claims of the House Comm. on the Judiciary*, 109th Cong., 1st Sess. (Apr. 21, 2005) (Serial No. 109-23), at 17 (statement of Richard Skinner); letter from the Honorable Michael C. Polt, Acting Assistant Secretary, Legislative Affairs, U.S. Department of State, to Jon Kyl, Senator, U.S. Senate (Mar. 16, 2009) [hereinafter "Letter of Mar. 16, 2009"] ("The Department has worked closely with other concerned agencies to improve our ability to check the biographic and biometric information on visa applicants against terrorist watchlists and data bases. The Terrorist Screening Center maintains the Terrorist Screening Database (TSDB), which contains all the names of known or suspected terrorists (KSTs) who have been watchlisted. These names are shared with the Consular Lookout and Support System (CLASS), which is the name-based screening system against which all visa applicant names are checked prior to visa issuance. If there are fingerprints associated with any KSTs in the TSDB, those fingerprints are contained in both the Department of Homeland Security (DHS) IDENT fingerprints system and the FBI IAFIS fingerprint system. Visa applicant fingerprints are screened against both IDENT and IAFIS prior to visa issuance. If there is a photograph associated with any KSTs in the TSDB, the photo is shared with the Facial Recognition System of the Department of State. Photos of visa applicants are screened against the Facial Recognition System prior to visa issuance.").

⁹⁶ Hearing of May 2, 2007, at 3 (statement of Dianne Feinstein).

checked against terrorist watchlists and databases.⁹⁷ Facial recognition technology is already used to collect such information, and a transition to a ten-print fingerprint system from a two-print system was scheduled to be implemented by December, 2007.⁹⁸ Both technologies should facilitate more effective identification of persons applying for visas under false identities.⁹⁹ The State Department has also introduced a new e-passport that features an electronic chip containing a traveler's biographic and biometric data.¹⁰⁰

In addition to these new technologies, the State Department is using its human resources to combat document fraud and foster cooperative relationships at home and abroad. Consular officers abroad are "specially trained to observe demeanor and detect inconsistencies" when interviewing visa applicants, in order to detect inconsistencies that suggest document fraud.¹⁰¹ Mr. Donovan testified that implementation of the State Department Bureau of Diplomatic Security's (DS) Visa and Passport Strategic Plan, an initiative aimed at detecting and disrupting terrorist efforts to use fraudulent travel documents, would require additional DS personnel at "critical" posts around the world, as well as increased resources to facilitate data-sharing and cooperation with foreign partners.¹⁰² Mr. Donovan further testified that DS, which has a presence in 159 countries, expects to have 33 special agents at "key posts" abroad by the end of 2007, and 50 by the end of 2008.¹⁰³

⁹⁷ Hearing of May 2, 2007, at 6 (statement of Andrew Simkin).

⁹⁸ Hearing of May 2, 2007, at 6 (statement of Andrew Simkin); letter of Mar. 16, 2009 ("[S]ince the beginning of the Biometric Visa Program in 2004, we [the State Department] had been collecting two index fingerprints from visa applicants and clearing them through the DHS IDENT fingerprint system. Throughout 2007, consular offices at posts around the world transitioned fingerprint collection from visa applicants from two prints to ten prints. As a result, on January 2, 2008, in addition to fingerprint clearance through IDENT, we began clearing all visa applicant ten prints through the FBI IAFIS fingerprint system. The addition of the fingerprint clearance through IAFIS has helped enforce compliance with the provision in the Immigration and Nationality Act (INA) that a person who has committed a crime involving moral turpitude is ineligible for a visa. In 2008, the fingerprints of 7,660,791 visa applicants were sent to IAFIS, resulting in the return of 52,777 criminal history records to consular officers adjudicating the visa applications. The availability of these criminal history records helped the consular officers adjudicate the visa applications in compliance with the INA provision regarding crimes involving moral turpitude.").

⁹⁹ Hearing of May 2, 2007, at 6 (statement of Andrew Simkin).

¹⁰⁰ Hearing of May 2, 2007, at 6 (statement of Andrew Simkin); *id.* at 33 (statement of Paul Morris).

¹⁰¹ Hearing of May 2, 2007, at 6 (statement of Andrew Simkin).

¹⁰² Hearing of May 2, 2007, at 8 (statement of Patrick Donovan).

¹⁰³ Hearing of May 2, 2007, at 8 (statement of Patrick Donovan).

Forensic Documents Laboratory

At DHS, the U.S. Immigration Customs and Enforcement Forensic Documents Laboratory (FDL) is “dedicated exclusively to fraudulent document detection and deterrence.”¹⁰⁴ In addition to publishing alerts and reports about fraudulent documents for law enforcement agencies across the globe,¹⁰⁵ the FDL also provides real-time support to field personnel worldwide, allowing potentially fraudulent documents to be remotely verified.¹⁰⁶

The FDL is also developing higher quality and more secure documents.¹⁰⁷ Technological advances continue to make high-quality fraudulent documents easier to produce and harder to detect. As a consequence, legitimate producers and issuers of travel and identity documents must constantly strive to make such documents more secure.¹⁰⁸ The FDL provides support for these efforts¹⁰⁹ and conducts fraudulent document recognition and training programs for domestic and foreign law enforcement personnel stationed at various posts around the globe.¹¹⁰ The FDL is thus engaged on a global scale in the effort to make travel documents more secure and to identify fraudulent documents when they are used.

Western Hemisphere Travel Initiative

Recognizing that the “standardization of travel documents is a critical step to securing our Nation’s borders,”¹¹¹ Congress has mandated the Western Hemisphere Travel Initiative (WHTI). The initiative, which “requires all citizens of the United States, Canada, Mexico, and Bermuda to have a passport or other accepted document that establishes the bearer’s identity and nationality to enter or reenter the United States from within the Western Hemisphere,”¹¹² is being jointly implemented by the

¹⁰⁴ Hearing of May 2, 2007, at 9 (statement of Michael Everitt).

¹⁰⁵ Hearing of May 2, 2007, at 10 (statement of Michael Everitt).

¹⁰⁶ Hearing of May 2, 2007, at 11 (statement of Michael Everitt).

¹⁰⁷ Hearing of May 2, 2007, at 10 (statement of Michael Everitt).

¹⁰⁸ Hearing of May 2, 2007, at 10 (statement of Michael Everitt).

¹⁰⁹ Hearing of May 2, 2007, at 10 (statement of Michael Everitt).

¹¹⁰ Hearing of May 2, 2007, at 10 (statement of Michael Everitt).

¹¹¹ Hearing of May 2, 2007, at 12 (statement of Paul Morris).

¹¹² Department of Homeland Security, *Western Hemisphere Travel Initiative: The Basics*, <http://www.dhs.gov/xtrlvsec/crossingborders/whitbasics.shtm> (last visited June 8, 2007).

Departments of State and Homeland Security. The initial phase of the WHTI, which requires all air travelers entering the United States to have passports or other valid travel documents, went into effect in January 2007.¹¹³ Mr. Simkin testified that as a result of the WHTI's implementation, passport demand has risen sharply.¹¹⁴ Due to a backlog in passport applications, the second phase of the WHTI, which requires all travelers by land or sea to present a valid travel document, has been postponed from its original implementation date of January 1, 2008, until at least the summer of 2008.¹¹⁵ Instead, beginning January 31, 2008, travelers crossing U.S. borders by land or sea will be required to present proof of citizenship and an identity card, such as a driver's license, at their first entry.¹¹⁶

Another example of interagency cooperation to secure U.S. borders is an effort "to facilitate cross-border travel for U.S. citizens while enhancing the security of our citizens and travelers."¹¹⁷ Working together, the Departments of State and Homeland Security have proposed issuing a People Access Security Services (PASS) card to travelers as part of the WHTI. The card will be implemented as early as January 2008.¹¹⁸ Mr. Simkin acknowledged that neither the PASS cards nor the technology

¹¹³ Hearing of May 2, 2007, at 13 (statement of Paul Morris).

¹¹⁴ Hearing of May 2, 2007, at 20 (statement of Andrew Simkin).

¹¹⁵ Spencer S. Hsu and William Branigin, *New Passport Rules Postponed for at Least Six Months*, WASH. POST, June 21, 2007, at A11.

¹¹⁶ Spencer S. Hsu and William Branigin, *New Passport Rules Postponed for at Least Six Months*, WASH. POST, June 21, 2007, at A11; Department of Homeland Security Press Room, *Fact Sheet: DHS End-of-Year Accomplishments*, http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm (last visited Mar. 5, 2009) ("Compliance with Western Hemisphere Travel Initiative (WHTI) requirements for air travel currently exceeds 99 percent. DHS will implement similar secure document requirements for land and sea travel in June 2009. New procedures at land and sea ports of entry implemented in January 2008 ended acceptance of oral declarations alone and significantly reduced the types of acceptable documents to further secure our borders. This year, WHTI reader equipment using RFID technology is being installed at land ports of entry covering 95 percent of traffic volume and is revolutionizing border processing. DHS improved the standards of its identification cards in 2008 and is offering more secure Trusted Traveler Program and Lawful Permanent Resident Cards that include technology to help speed border crossings.").

¹¹⁷ Department of Homeland Security Press Room, *Fact Sheet: Western Hemisphere Travel Initiative (WHTI) Passport Card Technology Choice: Vicinity RFID*, http://www.dhs.gov/xnews/releases/pr_1161115330477.shtm (last visited June 27, 2007).

¹¹⁸ Hearing of May 2, 2007, at 13 (statement of Paul Morris); email from Ted Lovett, Associate Director, Office of Legislative Affairs, Department of Homeland Security, to Tom Humphrey, Legislative Aide, Senate Judiciary Committee (Mar. 3, 2009, 08:39:00 EST) (on file with author or recipient) ("[I]n addition to the Passport Card, other WHTI-compliant documents like the TTCs (NEXUS, FAST and SENTRI) and EDLs are also being produced and are what was referred to as PASS. We [the Department of Homeland Security] are continuing to work with states, the CBSA and tribal authorities on potential other cards that would be considered WHTI-compliant. Washington State started issuing EDLs in January 2008 and other states have

DHS intends to use to read the cards has been tested in a “true border environment.”¹¹⁹ Mr. Morris indicated that DHS is “actively engaged” with the state of Washington in assessing that state’s pilot project using driver’s licenses to achieve the same goals as the PASS card.¹²⁰

Stolen and Lost Travel Document System

The Department of Homeland Security, through Customs and Border Patrol (CBP), is also working with Interpol to implement the Stolen and Lost Travel Document system (SLTD). For each stolen or lost passport reported by participating countries, the SLTD database includes the passport number, issuing country, whether the passport was blank, and the date of the reported theft or loss. This system “enables law enforcement anywhere in the world to instantly run a check against the SLTD database. With one single swipe a border control officer can verify if a document is reported stolen or lost nationally and internationally.”¹²¹ Once fully implemented, the United States will be the first “major country to use the SLTD as an integrated prescreening tool.”¹²² Mr. Noble likened Interpol’s approach to “tripwires interconnected around the globe and in the paths of terrorists and other dangerous criminals.”¹²³ The system has grown significantly in the past five years. Today, 123 countries report their data, up from just 12 in 2002. In the same period, the number of registered documents has increased from 3,000 to more than 14 million.¹²⁴

Despite these gains, Mr. Noble argued, misplaced skepticism about Interpol’s system has caused “intractable” resistance in the United States and elsewhere to using information from law enforcement agencies around the world. In view of the positive results the SLTD has produced in Switzerland and the Caribbean countries, Mr. Noble urged the United States not only to implement the system, but also to advocate that

followed suit in 2008 (NY, VT). We anticipate Michigan to commence shortly; Arizona is moving in the same direction. TTCs have been issued for years.”).

¹¹⁹ Hearing of May 2, 2007, at 19 (statement of Andrew Simkin).

¹²⁰ Hearing of May 2, 2007, at 22 (statement of Paul Morris).

¹²¹ Interpol Media Releases, *Interpol Warns of Terrorists Using Stolen Travel Documents to Evade Detection*, <http://www.interpol.int/Public/ICPO/PressReleases/PR2007/PR200715.asp> (last visited June 28, 2007).

¹²² Hearing of May 2, 2007, at 12 (statement of Paul Morris).

¹²³ Hearing of May 2, 2007, at 25 (statement of Ronald K. Noble).

¹²⁴ Hearing of May 2, 2007, at 30 (statement of Ronald K. Noble).

other countries do so.¹²⁵ Mr. Morris testified that CBP will test an integrated border inspection system with a real-time Interpol connection in fall 2007.¹²⁶ CBP anticipated a pilot test in the second or third quarter of 2007 and “immediate implementation [of the system] after the pilot.”¹²⁷ CBP reported that it “[b]egan implementation of the Advance Passenger Information System (APIS) Interpol Interface implementation on October 15, 2007.”¹²⁸ Additionally, CBP “[i]mplemented [i]nitial [o]perating [c]apability for the Electronic System for Travel Authorizations (ESTA) on time on July 31, 2008.”¹²⁹

Mr. Noble also recommended requiring that airlines or airline reservation companies send the U.S. government the passport numbers of travelers seeking to board a plane or book a flight reservation.¹³⁰ Airline passengers’ passport numbers are transmitted and checked against the SLTD system by CBP within 15 minutes after a flight’s departure, and a rule change has been proposed that would require that this information be transmitted before departure.¹³¹ Mr. Noble, however, argued that the information should be obtained as soon as a traveler makes a reservation, so that law enforcement agencies might have greater opportunities for investigation.¹³² Under this proposal, the information would be transmitted from the airlines to Interpol, and then directly to the law enforcement agencies on the ground to determine what further action to take.¹³³ Mr. Ervin noted that in 2005, the Air Transport Association and Association of European Airlines offered to make passenger manifests available to DHS at the time of passenger check-in, typically two to three hours before take-off. DHS has not

¹²⁵ Hearing of May 2, 2007, at 26 (statement of Ronald K. Noble).

¹²⁶ Hearing of May 2, 2007, at 15 (statement of Paul Morris).

¹²⁷ Hearing of May 2, 2007, at 15 (statement of Paul Morris).

¹²⁸ Customs and Border Patrol, Securing America’s Borders - CBP 2008 Fiscal Year in Review, http://www.cbp.gov/xp/cgov/newsroom/highlights/08year_review.xml (last visited Feb. 19, 2009).

¹²⁹ Customs and Border Patrol, Securing America’s Borders - CBP 2008 Fiscal Year in Review, http://www.cbp.gov/xp/cgov/newsroom/highlights/08year_review.xml (last visited Feb. 19, 2009) (“ESTA provides on-line processing for Visa Waiver Program travelers, and is a web-based system which has the capability to collect biographic data, screen the data against the terrorist lookout including No-Fly list, Visa Revocations, and Interpol’s Lost and Stolen Travel Documents.”).

¹³⁰ Hearing of May 2, 2007, at 34 (statement of Ronald K. Noble).

¹³¹ Hearing of May 2, 2007, at 34 (statement of Mr. Bartoldus).

¹³² Hearing of May 2, 2007, at 34 (statement of Ronald K. Noble).

¹³³ Hearing of May 2, 2007, at 35 (statement of Ronald K. Noble).

accepted either institution's offer, but Mr. Ervin argued that it would be advisable to do so.¹³⁴

Potential Vulnerabilities: The Visa Waiver Program

Although efforts are underway at the State Department and DHS to detect and deter document fraud, the Subcommittee believes that weaknesses in security remain and must be addressed. One such potential vulnerability is from the Visa Waiver Program (VWP), which allows travelers from participating countries to spend 90 days in the country without a visa.¹³⁵ Senator Feinstein argued that the VWP, under which approximately 15 million people enter the United States each year, is the "soft underbelly of this Nation,"¹³⁶ as travelers from countries participating in the program are generally subjected to far less scrutiny than those from countries that do not participate. Mr. Ervin noted that nearly all non-visa waiver travelers are interviewed by consular officers conversant in their languages and familiar with their customs, whereas visitors from visa waiver countries are typically interviewed only briefly at ports of entry, usually by inspectors who speak only English.¹³⁷ Additionally, more biographic and biometric information is collected about travelers from non-visa waiver countries, making it easier to verify travelers' identities.¹³⁸

Stolen passports from visa waiver countries also pose a serious problem, Mr. Ervin testified.¹³⁹ Of the 6.7 million passports in Interpol's database, 2.7 million are from visa waiver countries.¹⁴⁰ According to the Government Accountability Office's findings, between January and June 2005, 298 stolen passports from visa waiver countries were used to try to enter the United States.¹⁴¹

Given these shortcomings, Mr. Ervin advocated doing away with the VWP, a change which "need not hurt tourism, trade, and our international image."¹⁴² In its

¹³⁴ Hearing of May 2, 2007, at 35 (statement of Clark Kent Ervin).

¹³⁵ Hearing of May 2, 2007, at 13 (statement of Paul Morris).

¹³⁶ Hearing of May 2, 2007, at 23 (statement of Dianne Feinstein).

¹³⁷ Hearing of May 2, 2007, at 27 (statement of Clark Kent Ervin).

¹³⁸ Hearing of May 2, 2007, at 27 (statement of Clark Kent Ervin).

¹³⁹ Hearing of May 2, 2007, at 27 (statement of Clark Kent Ervin).

¹⁴⁰ Hearing of May 2, 2007, at 30 (statement of Ronald K. Noble).

¹⁴¹ Hearing of May 2, 2007, at 27 (statement of Clark Kent Ervin).

¹⁴² Hearing of May 2, 2007, at 27 (statement of Clark Kent Ervin).

place, Mr. Ervin suggested increasing the State Department's funding in order to hire more consular officers to process visa applications, so that travelers from current visa waiver countries would not need to face delays in obtaining visas.¹⁴³ Mr. Noble, in contrast, suggested that an "interim response," similar to the system used for reporting and cancelling lost credit cards, would be more appropriate. Under his proposal, all countries would be required to report the theft of blank passports and upload that information to an international database.¹⁴⁴ Mr. Zimmer, too, urged against eliminating the VWP and suggested instead that the United States take full advantage of the Immigration Advisory Program (IAP) to identify high-risk travelers.¹⁴⁵ The IAP, an initiative of the Department of Homeland Security, posts officers at "high-volume, high risk" airports overseas "to screen passengers before they board . . . aircraft destined for the U.S."¹⁴⁶ Since the program became operational, more than 1,200 passengers have been prevented from boarding U.S.-bound planes. The program continues to expand, and Mr. Zimmer indicated that it is proving effective at identifying persons carrying fraudulent documents as well as "high-risk travelers."¹⁴⁷

Conclusion

Fraudulent international travel documents pose a grave threat to the national security of the United States, and the federal government must respond to this threat effectively. The Departments of State and Homeland Security have undertaken a series of initiatives, including implementation of the WHTI and SLTD programs, aimed at securing United States travel documents and intercepting fraudulent documents at ports of entry. For instance, following the Subcommittee's hearing, DHS stated that "technology upgrades under the Western Hemisphere Travel Initiative (WHTI) were completed at land border crossings marking the start for new Radio Frequency Identification (RFID) technology deployments at 354 northern and southern border ports that account for 95 percent of all cross-border travel into the United States."¹⁴⁸ In December 2008, the DHS also suggested that "[c]ompliance with Western Hemisphere Travel Initiative (WHTI) requirements for air travel currently exceeds 99 percent" and

¹⁴³ Hearing of May 2, 2007, at 28 (statement of Clark Kent Ervin).

¹⁴⁴ Hearing of May 2, 2007, at 31 (statement of Ronald K. Noble).

¹⁴⁵ Hearing of May 2, 2007, at 29 (statement of Brian Zimmer).

¹⁴⁶ Hearing of May 2, 2007, at 13 (statement of Paul Morris).

¹⁴⁷ Hearing of May 2, 2007, at 29 (statement of Brian Zimmer).

¹⁴⁸ Department of Homeland Security, *Department of Homeland Security, Fact Sheet: DHS End-of-Year Accomplishments*, http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm (last visited Feb. 24, 2009).

that it “will implement similar secure document requirements for land and sea travel in June 2009.”¹⁴⁹

While these are all important steps, the Subcommittee’s hearing demonstrated that significant security gaps remain. To help curb the fraudulent use of travel documents, Senators Feinstein, Kyl, and Sessions sponsored the Passport and Visa Security Act, which would impose sentencing guidelines for a variety of offenses, including: (1) trafficking in passports; (2) making a false statement in an application for a passport; and (3) forgery or unlawful production of a passport.¹⁵⁰ In addition to legislative remedies, the Subcommittee will encourage continued interagency cooperation to respond proactively to existing travel document vulnerabilities and secure America’s borders.

Weaknesses in the Visa Waiver Program: Are the Needed Safeguards in Place to Protect America?

Introduction

People with permanent residence outside the United States, but who wish to visit the United States temporarily, typically must apply for a nonimmigrant visa. To obtain a nonimmigrant visa, a foreign national must submit an application for review by a United States consular officer at an American embassy or consulate. The officer reviews the application and, after interviewing the applicant, determines whether that individual is eligible to enter the United States.¹⁵¹

In 1986, the U.S. government began the Visa Waiver Program (VWP), which “enables nationals of certain countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa.”¹⁵² According to the Department of State, the VWP was established “with the objective of eliminating

¹⁴⁹ Department of Homeland Security, *Department of Homeland Security, Fact Sheet: DHS End-of-Year Accomplishments*, http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm (last visited Feb. 24, 2009).

¹⁵⁰ Passport and Visa Security Act of 2007, S. 276, 110th Cong. (2007) (the bill was referred to the Judiciary Committee but was not acted upon before the end of 110th Congress).

¹⁵¹ U.S. Department of State, *What is a Visa?*, <http://www.unitedstatesvisas.gov/whatis/index.html> (last visited Nov. 5, 2008).

¹⁵² U.S. Department of State, *Overview — What is the Visa Waiver Program?*, http://travel.state.gov/visa/temp/without/without_1990.html#vwp (last visited Nov. 5, 2008).

unnecessary barriers to travel, stimulating the tourism industry, and permitting the Department of State to focus consular resources in other areas.”¹⁵³ The VWP, which began as a pilot-program, was permanently authorized by the Visa Waiver Permanent Program Act in 2000.¹⁵⁴

At the time of the hearing, the VWP allowed foreign nationals from 27 countries¹⁵⁵ to enter the United States without a visa. According to Paul Rosenzweig, Assistant Secretary for International Affairs and Deputy Assistant Secretary for Policy at the Department of Homeland Security (DHS), almost 16 million foreign citizens entered the United States through the VWP in 2007.¹⁵⁶ Although the VWP has been praised for facilitating foreign travel and providing economic benefits, it has also been criticized for posing “inherent security, law enforcement, and illegal immigration risks to the United States.”¹⁵⁷ The VWP’s expedited entrance process, which allows foreign nationals from member countries to bypass interviews with United States consular officers, “could be exploited to gain illegal entry into the United States.”¹⁵⁸

On February 28, 2008, the Subcommittee convened a hearing entitled “Weaknesses in the Visa Waiver Program: Are the Needed Safeguards in Place to Protect America?” to investigate the VWP’s impact on our nation’s security. Specifically, the hearing addressed the findings of the Government Accountability Office (GAO)¹⁵⁹ concerning the Executive’s efforts to expand the VWP and its

¹⁵³ U.S. Department of State, *Overview — What is the Visa Waiver Program?*, http://travel.state.gov/visa/temp/without/without_1990.html#vwp (last visited Nov. 5, 2008).

¹⁵⁴ Visa Waiver Permanent Program Act, Pub. L. No. 106-396 (2000).

¹⁵⁵ The participating countries are Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

¹⁵⁶ *Weaknesses in the Visa Waiver Program: Are the Needed Safeguards in Place to Protect America?: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 2d Sess. (Feb. 28, 2008) (S. Hrg. 110-473, Serial No. J-110-77), at 18 (statement of Paul Rosenzweig) [hereinafter “Hearing of Feb. 28, 2008”].

¹⁵⁷ *The Visa Waiver Program: Mitigating Risks to Ensure Safety of All Americans: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 2d Sess. (Sept. 24, 2008) (S. Hrg. 110-674, Serial No. J-110-121), at 5 (statement of Jess Ford).

¹⁵⁸ Hearing of Feb. 28, 2008, at 101 (written statement of Jess Ford).

¹⁵⁹ GAO, *Visa Waiver Program: Limitations with Department of Homeland Security’s Plan to Verify Departure of Foreign Nationals*, GAO-08-458T (Washington, D.C., Feb. 28, 2008).

compliance with relevant provisions of the “Implementing Recommendations of the 9/11 Commission Act of 2007” (9/11 Act).¹⁶⁰

Five experts testified at the hearing: (1) Paul Rosenzweig, Deputy Assistant Secretary, Office of Policy, Department of Homeland Security; (2) Tony Edson, Deputy Assistant Secretary for Visa Services, Department of State; (3) Jess Ford, Director, International Affairs and Trade, Government Accountability Office; (4) Susan Ginsburg, Director of Programs on Mobility and Security, Migration Policy Institute; and (5) Jessica Vaughn, Senior Policy Analyst, Center for Immigration Studies.

VWP Vulnerabilities

At the Subcommittee hearing, Senator Feinstein warned that the VWP is the “soft underbelly” of our country because it “leaves open both a major gap in our domestic security and a way to exploit and countervene our immigration laws.”¹⁶¹

The gap in domestic security is the result of the VWP’s expedited entrance process, which Senator Feinstein characterized as “an attractive option to terrorists looking to do Americans harm.”¹⁶² As DHS Secretary Michael Chertoff has pointed out, the “first time we encounter [VWP travelers] is when they arrive at the United States, and that creates a very small window of opportunity to check them out.”¹⁶³ Senator Feinstein reinforced this concern by noting that both Richard Reid,¹⁶⁴ the “Shoe Bomber,” and Zacarias Moussaoui¹⁶⁵ entered the United States through the VWP.¹⁶⁶ Secretary Michael Chertoff has also stated that DHS is increasingly concerned about

¹⁶⁰ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 711, 121 Stat. 266, 338-345 (2007).

¹⁶¹ Hearing of Feb. 28, 2008, at 2 (statement of Dianne Feinstein).

¹⁶² Hearing of Feb. 28, 2008, at 2 (statement of Dianne Feinstein).

¹⁶³ BBC News Player, *Threat ‘will come from Europe,’* http://news.bbc.co.uk/player/nol/newsid_7190000/newsid_7191200/7191275.stm?bw=bb&mp=wm&asb=1&news=1&ms3=54&ms_javascript=true&bbcws=2 (last visited Nov. 5, 2008).

¹⁶⁴ Richard Reid is commonly known as the “Shoe Bomber” for his attempt to blow up American Airlines Flight #63 by detonating plastic explosives in his shoes. He was convicted and is serving a life sentence at a Supermax prison in Colorado.

¹⁶⁵ Zacarias Moussaoui is often referred to as the “20th Hijacker.” He is the only person charged in connection with the September 11, 2001, attacks and is currently serving a life sentence at a Supermax prison in Colorado.

¹⁶⁶ Hearing of Feb. 28, 2008, at 16 (statement of Dianne Feinstein).

“the possibility of Europe becoming a platform for a threat against the United States.”¹⁶⁷ This is particularly relevant to the VWP, because the program “allows most Europeans . . . to travel without a visa” to the United States.¹⁶⁸

The VWP has also been criticized for contributing to illegal immigration. It is estimated that as many as 40 percent of all illegal immigrants in the United States have overstayed their visas,¹⁶⁹ that is, entered the country legally but remained in the United States beyond their required departure dates. According to Ms. Vaughan, these overstays cost America roughly three to five billion dollars a year.¹⁷⁰ Senator Feinstein stated that of the 40 percent of illegal immigrants who overstay, hundreds of thousands likely came to the United States through the VWP.¹⁷¹ Once those individuals have entered the United States, it is easy for them to “simply disappear into the shadows.”¹⁷²

The federal government is unable to identify those who have overstayed. According to Mr. Ford, “[t]he inability of the U.S. Government to track the status of foreign nationals who arrive in the United States, to identify those that have overstayed their authorized period of visit and may still be in the United States, and to use these data to compute overstay rates has been a longstanding weakness in the oversight of the Visa Waiver Program.”¹⁷³ That, coupled with the limited capability of Immigration and Customs Enforcement (ICE), has stymied enforcement efforts and made it difficult to track down and remove more than a fraction of our nation’s illegal population.¹⁷⁴

Despite the numerous security challenges presented by the VWP, Mr. Rosenzweig, Deputy Assistant Secretary of the Office of Policy at DHS, affirmed the Administration’s commitment to the VWP, stating that “[t]he Department supports a

¹⁶⁷ BBC News Player, *Threat ‘will come from Europe,’* http://news.bbc.co.uk/player/nol/newsid_7190000/newsid_7191200/7191275.stm?bw=bb&mp=wm&asb=1&news=1&ms3=54&ms_javascript=true&bbcws=2 (last visited Nov. 5, 2008).

¹⁶⁸ BBC News Player, *Threat ‘will come from Europe,’* http://news.bbc.co.uk/player/nol/newsid_7190000/newsid_7191200/7191275.stm?bw=bb&mp=wm&asb=1&news=1&ms3=54&ms_javascript=true&bbcws=2 (last visited Nov. 5, 2008).

¹⁶⁹ Hearing of Feb. 28, 2008, at 12 (statement of Susan Ginsburg).

¹⁷⁰ Hearing of Feb. 28, 2008, at 13 (statement of Jessica Vaughan).

¹⁷¹ Hearing of Feb. 28, 2008, at 1 (statement of Dianne Feinstein).

¹⁷² Hearing of Feb. 28, 2008, at 1 (statement of Dianne Feinstein).

¹⁷³ Hearing of Feb. 28, 2008, at 10 (statement of Jess Ford).

¹⁷⁴ Hearing of Feb. 28, 2008, at 14 (statement of Jessica Vaughan) (ICE is only capable of removing roughly 250,000 people a year).

Visa Waiver Program that promotes legitimate travel to the United States without compromising, and in our judgment even strengthening, our country's national security, law enforcement, and immigration interests.”¹⁷⁵

Section 711 of the 9/11 Commission Act

Section 711 of the 9/11 Act, which was signed into law in August 2007, sought to “modernize and strengthen the security” of the VWP.¹⁷⁶ Prior to the 9/11 Act, countries entering the VWP needed: (1) a refusal rate of less than three percent during the previous fiscal year; or (2) an average refusal rate¹⁷⁷ of less than two percent in the previous two fiscal years, and a single year refusal rate of less than two and a half percent in one of those years.¹⁷⁸ The 9/11 Act provides DHS with the authority to waive those requirements and admit countries to the VWP if they have visa refusal rates of less than 10 percent in the previous fiscal year.¹⁷⁹ However, before exercising the 9/11 Act's VWP waiver authority, the Secretary of DHS must certify that: (1) “an air exit system is in place that can verify the departure of not less than 97 percent of foreign nationals who exit through airports of the United States”; and (2), “the electronic travel authorization system . . . is fully operational.”¹⁸⁰

After those certifications have been made, the Secretary of DHS, in consultation with the Secretary of State, can exercise the waiver authority, if (1) the Secretary of DHS determines that the totality of the country's security measures provides assurance that the country's participation in the program would not compromise the immigration laws of the United States;¹⁸¹ (2) there has been a consistent reduction in the country's refusal rate and conditions exist so that the refusal rate will continue to decline;¹⁸² (3) the country has cooperated on counterterrorism initiatives, information sharing, and preventing terrorist travel, and the Secretary of DHS and the Secretary of State have

¹⁷⁵ Hearing of Feb. 28, 2008, at 5 (statement of Paul Rosenzweig).

¹⁷⁶ Pub. L. No. 110-53, § 711(b), 121 Stat. 266, 338 (2007).

¹⁷⁷ The refusal rate refers to visa applications that are denied as a percentage of the total temporary visa applications for nationals of that country.

¹⁷⁸ Immigration and Nationality Act, 8 U.S.C.A. § 1187(c)(2)(A) (West 2007).

¹⁷⁹ Pub. L. No. 110-53, § 711(c), 121 Stat. 266, 339 (2007).

¹⁸⁰ Pub. L. No. 110-53, § 711(c), 121 Stat. 266, 339 (2007).

¹⁸¹ Immigration and Nationality Act, 8 U.S.C.A. § 1187(c)(8)(B)(ii) (West 2007).

¹⁸² Immigration and Nationality Act, 8 U.S.C.A. § 1187(c)(8)(B)(iii) (West 2007).

determined that such cooperation will continue;¹⁸³ and (4) the country's visa refusal rate during the previous year was not greater than 10 percent or, alternatively, the overstay rate for the previous year does not exceed the maximum overstay rate,¹⁸⁴ which is determined by the two secretaries.¹⁸⁵

According to Mr. Rosenzweig, the 9/11 Act enhances the VWP's security requirements and creates "flexibility that expands opportunities for new countries to join the Visa Waiver Program while imposing new security requirements on existing visa waiver countries."¹⁸⁶ Mr. Edson, Deputy Assistant Secretary for Visa Services at the Department of State, agreed, stating that the act "creates a path for expansion of the program to include some of our closest allies," and will "secure U.S. borders" and "promote a safer international travel environment."¹⁸⁷

Certifying the Air Exit Requirement: A Flawed Methodology

The 9/11 Act directs the Secretary of DHS to certify to Congress in writing when an exit system is in place that can verify the departure of 97 percent of foreign nationals who leave the United States by air.¹⁸⁸ At the hearing, Mr. Ford leveled several criticisms against DHS's proposed methodology for certifying this exit requirement. According to Mr. Ford, DHS plans to start with departure records, which "will not inform the overall and country-specific overstay rates — key factors in determining illegal immigration and security risks in the Visa Waiver Program."¹⁸⁹ Moreover, the methodology relies on airline departure data, which are of questionable accuracy.¹⁹⁰ According to Mr. Ford, a person listed on airline records as having departed may not have left, and some who do leave may be absent from those records.¹⁹¹

¹⁸³ Immigration and Nationality Act, 8 U.S.C.A. § 1187(c)(8)(B)(iv) (West 2007).

¹⁸⁴ Hearing of Feb. 28, 2008, at 104 (written statement of Jess Ford) ("The overstay rate is the ratio of the total number of nationals of a country who were admitted to the United States as nonimmigrant visitors during the previous fiscal year, and who violated the terms of such admission by remaining in the country beyond the authorized time period, to the total number of nationals of that country who arrived at a U.S. port-of-entry, and applied for admission into the United States as nonimmigrant visitors during the same period.").

¹⁸⁵ Pub. L. No. 110-53, § 711(c), 121 Stat. 266, 339 (2007).

¹⁸⁶ Hearing of Feb. 28, 2008, at 5 (statement of Paul Rosenzweig).

¹⁸⁷ Hearing of Feb. 28, 2008, at 7 (statement of Tony Edson).

¹⁸⁸ Pub. L. No. 110-53, § 711(c), 121 Stat. 266, 339 (2007).

¹⁸⁹ Hearing of Feb. 28, 2008, at 9 (statement of Jess Ford).

¹⁹⁰ Hearing of Feb. 28, 2008, at 109 (written statement of Jess Ford).

¹⁹¹ Hearing of Feb. 28, 2008, at 109 (written statement of Jess Ford).

In response to questions from Senator Feinstein, Mr. Rosenzweig explained that the methodology under consideration by DHS would not verify the departure of 97 percent of those who entered the country; rather, it would verify with 97 percent accuracy that departing visitors actually leave the country.¹⁹² Mr. Rosenzweig's response affirmed GAO's findings and suggested that DHS would, in fact, utilize a methodology that failed to track visitors from the time of their arrival, thereby proving of little use in determining the number of overstay.¹⁹³

In responding to these criticisms, Mr. Rosenzweig emphasized that DHS had not decided which methodology it would use to make the 97 percent air exit certification.¹⁹⁴ Senator Kyl asked Mr. Rosenzweig to communicate to Secretary Chertoff that a system based on departures is not an appropriate means of compliance with the law.¹⁹⁵

VWP Expansion

In 2005, DHS began negotiations with thirteen "roadmap" countries in preparation for the next wave of the VWP admissions. According to Senator Feinstein, seven¹⁹⁶ of the thirteen countries exceed the maximum ten percent refusal rate set forth under the 9/11 Act's VWP waiver provisions.¹⁹⁷ She questioned the prudence of admitting some of these roadmap countries, specifically Romania, which has agreements with surrounding nations that only requires residency for 24 hours before allowing VWP travel and boasts a visa refusal rate of more than 35 percent, far exceeding the allowable limit.¹⁹⁸

Ms. Vaughan criticized the expansion effort and warned that "DHS is moving forward to add too many countries too quickly before it can show that it can even gauge the risks, much less manage them, and before we have a robust interior enforcement system in place to minimize the cost of the inevitable increases in crime and illegal immigration that will come from people taking advantage of the expansion of the

¹⁹² Hearing of Feb. 28, 2008, at 16, 21-24 (statement of Paul Rosenzweig).

¹⁹³ Hearing of Feb. 28, 2008, at 16, 21-24 (statement of Paul Rosenzweig).

¹⁹⁴ Hearing of Feb. 28, 2008, at 21 (statement of Paul Rosenzweig).

¹⁹⁵ Hearing of Feb. 28, 2008, at 24 (statement of Jon Kyl).

¹⁹⁶ Hearing of Feb. 28, 2008, at 16 (statement of Dianne Feinstein) (refusal rate percentages: Hungary 10.3, Latvia 11.8, Slovakia 12.0, Lithuania 12.9, Bulgaria 14.3, Poland 25.2, and Romania 37.7).

¹⁹⁷ Hearing of Feb. 28, 2008, at 16 (statement of Dianne Feinstein).

¹⁹⁸ Hearing of Feb. 28, 2008, at 16 (statement of Dianne Feinstein).

program.”¹⁹⁹ Senator Kyl reached a similar conclusion, stating that “until we have a system in place that at least offers the potential to identify how many and who the individuals are that overstay, it seems to me that we are moving too fast and, frankly, in potential violation of the law.”²⁰⁰

GAO Recommendations

The proposed methodology for certifying the 9/11 Act’s air exit system requirement, which is based on departure data, does not allow the federal government to determine overstay rates accurately, which is key to “determining illegal immigration and security risks in the Visa Waiver Program.”²⁰¹ Therefore, GAO recommends that DHS implement a system that uses “arrival data as a starting point and review[s] subsequent DHS records to determine whether these foreign nationals are still in the country.”²⁰² However, if DHS chooses to use a departure-based air exit system, GAO suggests making efforts to increase the accuracy of airlines’ departure data.²⁰³

Additionally, the United States does not have a land exit system.²⁰⁴ Consequently, even with a functioning air exit system, visitors could legally enter through a U.S. airport, exit legally by land to either Canada or Mexico, and their departure would not be recorded.²⁰⁵ Senator Kyl stated that “without a land exit system, our system will necessarily be incomplete.”²⁰⁶

¹⁹⁹ Hearing of Feb. 28, 2008, at 13 (statement of Jessica Vaughan).

²⁰⁰ Hearing of Feb. 28, 2008, at 16 (statement of Jon Kyl).

²⁰¹ Hearing of Feb. 28, 2008, at 9 (statement of Jess Ford).

²⁰² Hearing of Feb. 28, 2008, at 9 (statement of Jess Ford).

²⁰³ Hearing of Feb. 28, 2008, at 110 (written statement of Jess Ford).

²⁰⁴ Hearing of Feb. 28, 2008, at 18 (statement of Jon Kyl).

²⁰⁵ Hearing of Feb. 28, 2008, at 17 (statement of Paul Rosenzweig); *id.* at 27 (statement of Jeff Sessions) (during the hearing, Senator Sessions suggested that those who enter the United States by air be required to leave by air, or if they do not exit by air, that they be required to file documentation and a biometric fingerprint to verify their exit); *id.* at 27 (statement of Paul Rosenzweig) (Mr. Rosenzweig responded that that suggestion had been considered, but was not included in the final legislation. Mr. Rosenzweig expressed reservations about such a system).

²⁰⁶ Hearing of Feb. 28, 2008, at 18 (statement of Jon Kyl).

Conclusion

While the VWP fosters international goodwill and trade, it also poses national security and illegal immigration risks. These competing interests must be managed so that the VWP does not allow “people who would do us grievous injury to come to this country.”²⁰⁷ While an effective air exit system would help prevent abuse of the VWP, the ultimate goal of the United States should be a comprehensive exit system that tracks visitors as they enter and exit the United States by air, sea, or land.

Following the hearing, Senators Feinstein, Kyl, and Sessions wrote DHS Secretary Michael Chertoff to express their discontent with the methodology alluded to in Mr. Ford’s testimony.²⁰⁸ In that letter, the Senators suggested that adoption of the proposed methodology would be “unacceptable,” and emphasized that the purpose of the 9/11 Act was to create “an overstay system to track the arrivals and departures of visa waiver program travelers.”²⁰⁹ The proposed methodology, however, would fail to create such a system. According to Senators Feinstein, Kyl, and Sessions, any “methodology that ignores overstay data is ultimately meaningless.”²¹⁰

Secretary Chertoff responded to that letter six weeks later. In his response, he challenged the Senators’ interpretation of the 9/11 Act, arguing that their “reading is incompatible with the law.”²¹¹ He stated that the law only requires DHS to “verify the exit of 97% of foreign nationals who depart via air, not to verify the exit of 97% of those who enter the United States.”²¹²

The Secretary’s response, coupled with a follow-up report issued by the GAO, motivated a second hearing on the Executive’s efforts to expand the VWP and its compliance with the 9/11 Act on September 24, 2008.

²⁰⁷ Hearing of Feb. 28, 2008, at 28 (statement of Dianne Feinstein).

²⁰⁸ Letter from the Honorable Dianne Feinstein, Jon Kyl, and Jeff Sessions, Senators, U.S. Senate, to Michael Chertoff, Secretary of Homeland Security, U.S. Department of Homeland Security (Mar. 3, 2008) [hereinafter “Letter of Mar. 3, 2008”].

²⁰⁹ Letter of Mar. 3, 2008, at 1.

²¹⁰ Letter of Mar. 3, 2008.

²¹¹ Letter of Mar. 3, 2008.

²¹² Letter of Mar. 3, 2008, at 2.

The Visa Waiver Program: Mitigating Risks to Ensure Safety of All Americans

Introduction

On September 24, 2008, the Subcommittee convened a hearing to investigate ongoing concerns about the Visa Waiver Program (VWP), which allows foreign nationals from 27 countries to travel to the United States for up to 90 days without a visa.²¹³ Two experts on the VWP testified before the Subcommittee: (1) Stewart A. Baker, Assistant Secretary, Office of Policy, U.S. Department of Homeland Security (DHS), and (2) Jess T. Ford, Director of International Affairs and Trade, U.S. Government Accountability Office (GAO).

This hearing followed a February Subcommittee hearing²¹⁴ regarding a VWP report issued by GAO.²¹⁵ As a result of the information discussed at the February hearing, Senators Feinstein, Kyl, and Sessions initiated correspondence with DHS Secretary Michael Chertoff and requested another report from GAO, which was issued on September 15, 2008.²¹⁶ In this report, GAO reiterated concerns raised in its earlier report and the Subcommittee hearing about the Executive's planned expansion of the VWP and its compliance with relevant provisions of the "Implementing Recommendations of the 9/11 Commission Act of 2007" (the 9/11 Act).²¹⁷

²¹³ *The Visa Waiver Program: Mitigating Risks to Ensure Safety of All Americans: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 2d Sess. (Sept. 24, 2008) (S. Hrg. 110-674, Serial No. J-110-121), at 5 (statement of Jess Ford) [hereinafter "Hearing of Sept. 24, 2008"].

²¹⁴ *Weaknesses in the Visa Waiver Program: Are the Needed Safeguards in Place to Protect America?: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 2d Sess. (Feb. 28, 2008) (S. Hrg. 110-473, Serial No. J-110-77) [hereinafter "Hearing of Feb. 28, 2008"].

²¹⁵ GAO, *Visa Waiver Program: Limitations with Department of Homeland Security's Plan to Verify Departure of Foreign Nationals*, GAO-08-458T (Washington, D.C., Feb. 28, 2008).

²¹⁶ GAO, *Visa Waiver Program: Actions Are Needed to Improve Management of the Expansion Process, and to Assess and Mitigate Program Risks*, GAO-08-967 (Washington, D.C., Sept. 15, 2008) [hereinafter "GAO Rep. of Sept. 15, 2008"].

²¹⁷ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 338 (2007).

The Visa Waiver Program: Traditional Criticisms

The VWP is intended to facilitate trade and travel between member countries and the United States. Unlike other visitors, citizens of VWP countries may travel to the United States for up to 90 days without a visa.²¹⁸ These travelers are also not required to undergo pre-screening by a consular officer before departure. That lack of pre-screening makes it easier for criminals and terrorists to enter the United States undetected and, as a result, the VWP has been criticized for compromising U.S. national security.²¹⁹

The VWP has also been criticized for contributing to the number of individuals residing in the United States illegally. It is believed that, of those individuals residing in the United States illegally, 40 percent arrived legally but failed to depart when required to do so.²²⁰ The VWP offers an attractive opportunity for these individuals, known as “visa overstayers,” who exploit the program to gain legal entrance to the United States. Because the United States does not have an effective entry-exit system at its ports, law enforcement officials have a difficult time determining whether a particular VWP traveler has departed when required to do so, thereby facilitating overstays.²²¹

Balancing Competing Interests

Because of the VWP’s lack of pre-screening, participation is limited to countries whose foreign nationals are not believed to pose a significant threat to our national security. That threat is assessed, in part, based on a country’s “visa refusal rate,” a metric that reflects the ratio of (1) the number of individuals from that country who were refused a visa by the United States to (2) the number of individuals from that country who applied for visas.²²² Admittance to the VWP is usually limited to countries with visa refusal rates of less than three percent.²²³

²¹⁸ Immigration and Nationality Act, 8 U.S.C.A. § 1187(a)(1) (West 2007).

²¹⁹ Hearing of Sept. 24, 2008, at 1, 2-3, 24 (statement of Dianne Feinstein); *id.* at 9 (statement of Jon Kyl).

²²⁰ Hearing of Sept. 24, 2008, at 12 (statement of Dianne Feinstein).

²²¹ Hearing of Sept. 24, 2008, at 22-23 (statement of Stewart Baker).

²²² 8 U.S.C. § 1187(c)(A).

²²³ 8 U.S.C. § 1187(c)(A)(ii).

Several countries are interested in joining the VWP, and their admission would likely facilitate trade, travel, and advance positive diplomatic relations. However, their admission also raises national security concerns due to unfettered travel.²²⁴

The 9/11 Commission Act

Section 711 of the 9/11 Act makes a number of significant changes to the VWP. Most notably, it provides mechanisms by which the Secretaries of State and DHS may waive traditional requirements for VWP membership when seeking to admit new countries.²²⁵ However, before exercising the 9/11 Act's VWP waiver authority, the Secretary of DHS must certify that (1) "an air exit system is in place that can verify the departure of not less than 97 percent of foreign nationals who exit through airports of the United States" and (2) "the electronic travel authorization system . . . is fully operational."²²⁶

The Executive's Efforts to Expand the VWP

In 2005, DHS announced nine "roadmap" countries that would be considered for admission to the VWP.²²⁷ Since that time, DHS has actively worked with these countries to meet the minimum standards for VWP admittance.²²⁸ DHS hoped to admit eight before the end of 2008, seven of which have visa refusal rates that exceed the customary VWP standard of three percent. GAO has suggested that, to admit those seven countries in 2008, DHS intended to exercise the 9/11 Act's waiver authority, which permits the admittance of countries with visa refusal rates of up to 10 percent.²²⁹

Subcommittee Action on the Planned Expansion of the VWP

In its February 2008 hearing, the Subcommittee heard GAO's concerns about the Executive's proposed VWP expansion.²³⁰ GAO was wary about DHS's proposed

²²⁴ GAO Rep. of Sept. 15, 2008, at 2.

²²⁵ Pub. L. No. 110-53, § 711(c), 121 Stat. 266, 339 (2007).

²²⁶ Pub. L. No. 110-53, § 711(c), 121 Stat. 266, 339 (2007).

²²⁷ Hearing of Sept. 24, 2008, at 15 (statement of Stewart Baker).

²²⁸ Hearing of Sept. 24, 2008, at 15 (statement of Stewart Baker).

²²⁹ Pub. L. No. 110-53, § 711(c), 121 Stat. 266, 340 (2007).

²³⁰ *Weaknesses in the Visa Waiver Program: Are the Needed Safeguards in Place to Protect America?: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the*

method for certifying compliance with the 9/11 Act's air exit system requirement. Mr. Ford, testifying for GAO, explained that DHS intends to "match records of foreign nationals departing the country, as reported by airlines, to the department's existing records of any prior arrivals, immigration status changes, or prior departures from the United States."²³¹ According to DHS, with this method, "it can attain a match rate above 97 percent, based on August 2007 data, to certify compliance" with the 9/11 Act's air exit system requirement.²³² Paul Rosenzweig, who testified on behalf of DHS, acknowledged that this process was under consideration and that, in the view of DHS, it would be sufficient to meet the air exit system requirement.²³³ Although Mr. Rosenzweig assured the Subcommittee that DHS had not yet decided on a methodology for certifying the air exit system requirement, Senators Feinstein, Kyl, and Sessions expressed reservations about the methodology highlighted in Mr. Ford's testimony.²³⁴

As noted above, Senators Feinstein, Kyl, and Sessions wrote DHS Secretary Michael Chertoff expressing their dissatisfaction with the techniques described in Mr. Ford's testimony.²³⁵ Secretary Chertoff's response challenged the Senators' interpretation of the 9/11 Act,²³⁶ citing that the law only requires DHS to "verify the exit of 97% of foreign nationals who depart via air, not to verify the exit of 97% of those who enter the United States."²³⁷

GAO Findings

Five months after the exchange of correspondence between Secretary Chertoff and Senators Feinstein, Kyl, and Sessions, GAO released another report on the

Judiciary, 110th Cong., 2d Sess. (Feb. 28, 2008) (S. Hrg. 110-473, Serial No. J-110-77) [hereinafter "Hearing of Feb. 28, 2008"].

²³¹ Hearing of Feb. 28, 2008, at 100 (written statement of Jess Ford).

²³² Hearing of Feb. 28, 2008, at 100 (written statement of Jess Ford).

²³³ Hearing of Feb. 28, 2008, at 18 (statement of Paul Rosenzweig).

²³⁴ Letter from the Honorable Dianne Feinstein, Jon Kyl, and Jeff Sessions, Senators, U.S. Senate, to Michael Chertoff, Secretary of Homeland Security, U.S. Department of Homeland Security (Mar. 3, 2008) [hereinafter "Letter to Michael Chertoff from Dianne Feinstein, Jon Kyl, and Jeff Sessions"].

²³⁵ Letter to Michael Chertoff from Dianne Feinstein, Jon Kyl, and Jeff Sessions.

²³⁶ Letter from Michael Chertoff, Secretary of Homeland Security, U.S. Department of Homeland Security to the Honorable Dianne Feinstein, Jon Kyl, and Jeff Sessions, Senators, U.S. Senate, at 2 (Apr. 16, 2008) [hereinafter "Letter to Dianne Feinstein, Jon Kyl, and Jeff Sessions from Michael Chertoff"].

²³⁷ Letter to Dianne Feinstein, Jon Kyl, and Jeff Sessions from Michael Chertoff.

Executive's efforts to expand the VWP.²³⁸ In its report, GAO identified several areas of ongoing concern, including DHS's proposed methodology for the air-exit system, DHS's interpretation of a "fully operational" Electronic System for Travel Authorization,²³⁹ the accuracy and analysis of overstay data,²⁴⁰ biometric data collection,²⁴¹ lost and stolen passport reporting,²⁴² and information sharing among current and aspiring member countries.²⁴³

Certifying the 9/11 Act's Air Exit System Requirement

In its report, GAO reiterated its belief that DHS intends to use a flawed methodology to certify the 97 percent departure rate required by the 9/11 Act.²⁴⁴ According to GAO, DHS still intended to use the methodology discussed at the Subcommittee's February hearing, which would match airlines' departure records with those of travelers' prior arrivals, departures, or changes in immigration status.²⁴⁵ Senator Feinstein called this method "worthless,"²⁴⁶ and GAO concluded that it "will not help the department mitigate risks of the [VWP]"²⁴⁷ and "will not inform . . . overstay rates."²⁴⁸

Assistant Secretary Baker acknowledged that the proposed methodology "is not a measure of how many people have overstayed" and does not effectively match visitors' entry and exit.²⁴⁹ Nevertheless, he argued that it does fulfill the statutory requirement set forth in the 9/11 Act.²⁵⁰

²³⁸ GAO, *Visa Waiver Program: Actions Are Needed to Improve Management of the Expansion Process, and to Assess and Mitigate Program Risks*, GAO-08-967 (Washington, D.C., Sept. 15, 2008).

²³⁹ Hearing of Sept. 24, 2008, at 6 (statement of Jess Ford).

²⁴⁰ Hearing of Sept. 24, 2008, at 15 (statement of Jess Ford).

²⁴¹ Hearing of Sept. 24, 2008, at 20 (statement of Jess Ford).

²⁴² Hearing of Sept. 24, 2008, at 17-18 (statement of Jess Ford).

²⁴³ Hearing of Sept. 24, 2008, at 18 (statement of Jess Ford).

²⁴⁴ GAO Rep. of Sept. 15, 2008, at 16.

²⁴⁵ GAO Rep. of Feb. 28, 2008, at 7-11; GAO Rep. of Sept. 15, 2008, at 15-19.

²⁴⁶ Hearing of Sept. 24, 2008, at 12 (statement of Dianne Feinstein).

²⁴⁷ GAO Rep. of Sept. 15, 2008, at 15.

²⁴⁸ GAO Rep. of Sept. 15, 2008, at 16.

²⁴⁹ Hearing of Sept. 24, 2008, at 11 (statement of Stewart Baker).

²⁵⁰ Hearing of Sept. 24, 2008, at 12 (statement of Stewart Baker).

Senator Kyl agreed that the 9/11 Act's ambiguous wording left open the possibility of varying interpretations.²⁵¹ He also reminded Mr. Baker that while the statutory language might be unclear, Congress's intention should not be.²⁵² Congress intended for the 9/11 Act's waiver authority to be exercised only after the overstay issue had been addressed. DHS's methodology, however, would side-step the issue and do nothing to address overstays. As Senator Kyl stated, it is understandable that DHS thinks "it is valuable to generate the data on the effectiveness of the identification program, . . . [b]ut the real question, the big elephant in the room is the visa overstayers."²⁵³

Electronic System for Travel Authorization (ESTA)

The Electronic System for Travel Authorization (ESTA) is a prescreening tool that assesses the threat posed by a traveler prior to departure for the United States. ESTA operates by checking a traveler's biographic and other information against "law enforcement databases and watchlists."²⁵⁴ Because ESTA is used before travel commences, its deployment should help mitigate some of the national security concerns that arise due to the VWP's omission of prescreening by consular officers.

The 9/11 Act states that "[a]fter certification [of the air exit system and ESTA] by DHS Secretary, the Secretary, in consultation with the Secretary of State, may waive the application of [the visa refusal rate requirement]."²⁵⁵ DHS implemented ESTA on a voluntary basis on August 1, 2008;²⁵⁶ however, according to GAO, DHS has not yet provided a date on which it intends to certify that ESTA is "fully operational."²⁵⁷ DHS and Congress agree that ESTA must be "fully operational" before DHS may exercise the 9/11 Act's waiver authority.²⁵⁸ But DHS's interpretation of the phrase "fully

²⁵¹ Hearing of Sept. 24, 2008, at 13, 21 (statement of Jon Kyl).

²⁵² Hearing of Sept. 24, 2008, at 13 (statement of Jon Kyl).

²⁵³ Hearing of Sept. 24, 2008, at 14 (statement of Jon Kyl).

²⁵⁴ Hearing of Feb. 28, 2008, at 129 (written statement of Paul Rosenzweig); hearing of Sept. 24, 2008, at 8 (statement of Stewart Baker).

²⁵⁵ Pub. L. No. 110-53, § 711(c), 121 Stat. 266, 339 (2007).

²⁵⁶ Hearing of Sept. 24, 2008, at 6 (statement of Jess Ford).

²⁵⁷ Hearing of Sept. 24, 2008, at 6 (statement of Jess Ford).

²⁵⁸ GAO Rep. of Sept. 15, 2008, at 20 ("DHS attorneys tell [GAO] that the department could admit additional countries . . . once it provides [ESTA] certification"); hearing of Sept. 24, 2008 (transcript) (statement of Dianne Feinstein) ("law requires that before DHS admits any new countries into the [VWP], it must . . . put in place a fully operational [ESTA]").

operational” in the statute is limited and DHS’s ESTA certification did not take into account current VWP member countries.²⁵⁹

DHS acknowledges that it must certify ESTA and implement it in any aspirant country before that country can enter the VWP.²⁶⁰ However, DHS denies that ESTA must be fully implemented in *every* VWP country before *any* new member may be admitted.²⁶¹ In fact, DHS claims that ESTA is not required in current VWP countries until 60 days after final notice of the ESTA requirement is published in the Federal Register.²⁶² Based on the expected notification date, GAO estimates a deadline of January 12, 2009, for comprehensive implementation across all new and current VWP countries.²⁶³ GAO’s report states that DHS believes it may admit new countries with fully implemented ESTA until January 12, 2009, even if current VWP member countries have not adopted ESTA.²⁶⁴

Senator Feinstein challenged DHS’s interpretation of the ESTA requirement, suggesting that it is a “clear contradiction of the statute.”²⁶⁵ According to Senator Feinstein, the 9/11 Act should be read to require implementation of ESTA in all current countries before any new country can be admitted into the VWP.²⁶⁶

GAO has suggested that DHS’s plan to certify the system before the end of the year ignores obstacles to full implementation in aspirant countries.²⁶⁷ The hurdles to timely ESTA certification include (1) a lack of passenger awareness of the program; (2) the difficulty in coordinating with airlines; and (3) the State Department’s inability to manage an influx of visa requests from denied ESTA travelers.²⁶⁸

²⁵⁹ Hearing of Feb. 28, 2008, at 129 (statement of Paul Rosenzweig); *id.* at 3 (statement of Dianne Feinstein).

²⁶⁰ GAO Rep. of Sept. 15, 2008, at 20.

²⁶¹ GAO Rep. of Sept. 15, 2008, at 20.

²⁶² GAO Rep. of Sept. 15, 2008, at 20.

²⁶³ GAO Rep. of Sept. 15, 2008, at 4 n.7.

²⁶⁴ GAO Rep. of Sept. 15, 2008, at 20.

²⁶⁵ Hearing of Feb. 28, 2008, at 97 (written statement of Dianne Feinstein).

²⁶⁶ Hearing of Feb. 28, 2008, at 3 (statement of Dianne Feinstein).

²⁶⁷ Hearing of Sept. 24, 2008, at 6-7 (statement of Jess Ford).

²⁶⁸ Hearing of Sept. 24, 2008, at 7 (statement of Jess Ford).

Overstays

At the hearing, Senators Feinstein and Kyl and GAO expressed concern about VWP participants who overstay their visas. According to Senator Feinstein, VWP participants are “lost once they arrive,”²⁶⁹ and can easily remain in the United States without detection. Moreover, Senator Kyl and GAO emphasized that, in addition to identifying individuals who have remained in the United States illegally, overstay rates must be tracked to ensure that current VWP member countries are in compliance with the minimum standards for program participation.²⁷⁰

Information Sharing

Assistant Secretary Baker stated that DHS has already received commitments from several aspirant countries to share watchlist and lost or stolen passport information²⁷¹ and has expanded information sharing with these countries to include criminal convictions and potential terrorists.²⁷² He also stated that DHS wants similar commitments from all current VWP members.²⁷³ Senator Kyl emphasized the efficacy of a united legislative and executive front to encourage the sharing of security information, and suggested offering legislative incentives to current VWP member countries to provide this important information.²⁷⁴

Lost or Stolen Passports

Senators Feinstein and Kyl and GAO stressed the need for consistent, timely reporting of lost or stolen passports²⁷⁵ because a dangerous person with a lost or stolen passport from a VWP nation could enter the country unchecked.²⁷⁶ According to Assistant Secretary Baker, DHS has received commitments from aspiring member countries to report lost and stolen passports in a timely manner²⁷⁷ and is working toward

²⁶⁹ Hearing of Sept. 24, 2008, at 1 (statement of Dianne Feinstein); *id.* at 14 (statement of Jon Kyl).

²⁷⁰ Hearing of Sept. 24, 2008, at 4 (statement of Jon Kyl); *id.* at 6, 14 (statement of Jess Ford).

²⁷¹ Hearing of Sept. 24, 2008, at 7 (statement of Jess Ford); *id.* at 9 (statement of Stewart Baker).

²⁷² Hearing of Sept. 24, 2008, at 9 (statement of Stewart Baker).

²⁷³ Hearing of Sept. 24, 2008, at 18 (statement of Stewart Baker).

²⁷⁴ Hearing of Sept. 24, 2008, at 19 (statement of Jon Kyl).

²⁷⁵ Hearing of Sept. 24, 2008, at 2 (statement of Dianne Feinstein).

²⁷⁶ Hearing of Sept. 24, 2008, at 3, 24 (statement of Dianne Feinstein).

²⁷⁷ Hearing of Sept. 24, 2008, at 9 (statement of Stewart Baker).

a similar agreement with current VWP member countries.²⁷⁸ Under the law, however, current VWP member countries are not required to provide passport information.²⁷⁹ Though member countries may supply such information on a voluntary basis, GAO recommends formalizing agreements with current members to ensure full participation among all VWP countries.²⁸⁰

Concerns Regarding New Entrants and Visa Refusal Rates

Mr. Ford expressed concern that several of the countries that DHS is negotiating with for VWP admittance in 2008 have rejection rates that exceed 10 percent, the maximum permitted under the 9/11 Act's waiver provisions.²⁸¹ Mr. Ford noted that several of these countries are allies of the United States in Iraq and, therefore, have high expectations of gaining admission.²⁸² Assistant Secretary Baker explained that those countries' rates have steadily dropped,²⁸³ and DHS expects the rates for the most recent year to fall below the maximum, thereby making those countries eligible for admittance under the 9/11 Act's VWP waiver authority.²⁸⁴ Assistant Secretary Baker assured the Subcommittee that DHS does not intend to admit countries with refusal rates greater than 10 percent.²⁸⁵

Moving Forward

Senators Feinstein and Kyl, DHS, and GAO expressed a common desire to advance legislation that will close gaps in the VWP and make the program safer.²⁸⁶ However, despite the concerns expressed by Senators Feinstein and Kyl, the administration moved forward with its planned expansion of the Visa Waiver Program using its authority under the 9/11 Act. As a result, eight countries joined the VWP in 2008: the Czech Republic, Estonia, Hungary, the Republic of Korea, Latvia, Lithuania,

²⁷⁸ Hearing of Sept. 24, 2008, at 9 (statement of Stewart Baker).

²⁷⁹ Hearing of Sept. 24, 2008, at 6, 18 (statement of Jess Ford).

²⁸⁰ Hearing of Sept. 24, 2008, at 18 (statement of Jess Ford).

²⁸¹ Hearing of Sept. 24, 2008, at 6 (statement of Jess Ford).

²⁸² Hearing of Sept. 24, 2008, at 5 (statement of Jess Ford).

²⁸³ Hearing of Sept. 24, 2008, at 10 (statement of Stewart Baker); *id.* at 6 (statement of Jess Ford).

²⁸⁴ Hearing of Sept. 24, 2008, at 10 (statement of Stewart Baker); *id.* at 6 (statement of Jess Ford).

²⁸⁵ Hearing of Sept. 24, 2008, at 10 (statement of Stewart Baker).

²⁸⁶ Hearing of Sept. 24, 2008, at 4 (statement of Jon Kyl); *id.* at 50 (statement of Dianne Feinstein); *id.* at 9 (statement of Stewart Baker); *id.* at 18 (statement of Jess Ford).

Slovakia and Malta.²⁸⁷ Senators Feinstein and Kyl, believing that such an expansion relied on an interpretation of the 9/11 Act that undermines Congress' intent, introduced legislation in the 111th Congress that would require: (1) current visa waiver countries to report on lost or stolen visas in order to remain in the visa waiver program; (2) DHS and the State Department to perform an evaluation of member countries, including their overstay rates, and impose immediate suspension upon any that are noncompliant with existing limits; (3) DHS to verify 97 percent of VWP participants exiting and departing U.S. airports—based on arrival data, not just departure data, or else lose its waiver authority to further expand the visa waiver program; (4) the Secretary of DHS to compile all appropriate data to determine the visa overstay rate for each member country and sets a consistent maximum low visa overstay rate for all member countries; and (5) an audit of the electronic travel authorization system (ESTA).²⁸⁸

DOMESTIC SECURITY

Identity Theft: Innovative Solutions for an Evolving Problem

Introduction

Identity theft occurs when criminals illegally or improperly obtain and misuse sensitive, personally identifiable information.²⁸⁹ There are two types of identity theft: “the takeover or misuse of existing credit card, debit card, or other accounts (‘existing account fraud’); and the use of stolen information to open new accounts in the consumer’s name (‘new account fraud’).”²⁹⁰ Although new account fraud is less frequent, it “typically causes considerably more harm to consumers in out-of-pocket expenses and time necessary to repair the damage.”²⁹¹

²⁸⁷ Department of Homeland Security, *DHS Reminds Visa Waiver Program Travelers of ESTA Requirements Effective Today*, http://www.dhs.gov/xnews/releases/pr_1231771555521.shtm (last visited Mar. 5, 2009).

²⁸⁸ Strengthening the Visa Waiver Program to Secure America Act, S. 203, 111th Cong. (2009).

²⁸⁹ President’s Identity Theft Task Force, *Interim Recommendations* 1 (Sept. 2006), available at <http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf>.

²⁹⁰ *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 1st Sess. (Mar. 21, 2007) (S. Hrg. 110-62, Serial No. J-110-22), at 2-3 (written statement of Lydia Parnes) [hereinafter “Hearing of Mar. 21, 2007”].

²⁹¹ Hearing of Mar. 21, 2007, at 3 (written statement of Lydia Parnes).

For both Senators Feinstein and Kyl, combating identity theft has been a “top priority.”²⁹² In the past nine years, the Subcommittee has held eight hearings on identity theft in an effort to ensure the security and financial privacy of U.S. citizens and businesses.²⁹³ Senators Feinstein and Kyl’s leadership on this issue has led to the introduction and passage of important identity theft legislation,²⁹⁴ and in 2004, President Bush commended Senators Feinstein and Kyl for their leadership on the Identity Theft Penalty Enhancement Act.²⁹⁵

On March 21, 2007, the Subcommittee on Terrorism, Technology, and Homeland Security held a hearing to assess the efforts of the federal government and the states in combating identity theft. Two panels provided testimony at the hearing. Panel one consisted of (1) Lydia Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission; and (2) Ronald Tenpas, Associate Deputy Attorney General, Department of Justice. Panel two consisted of (1) James Davis, Chief

²⁹² *Identity Theft Penalty Enhancement Act of 2002: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 2nd Sess. (July 9, 2002) (S. Hrg. 107-900, Serial No. J-107-68), at 81 (statement of Dianne Feinstein).

²⁹³ *Database Security: Finding Out When Your Information Has Been Compromised: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108th Cong., 1st Sess. (Nov. 4, 2003) (S. Hrg. 108-520, Serial No. J-108-52); *Identity Theft Penalty Enhancement Act of 2002: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 2nd Sess. (July 9, 2002) (S. Hrg. 107-900, Serial No. J-107-68); *Identity Theft: Restoring Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 2nd Sess. (Mar. 20, 2002) (S. Hrg. 107-900, Serial No. J-107-68); *Privacy, Identity Theft, and the Protection of your Personal Information in the 21st Century: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 2nd Sess. (Feb. 14, 2002) (S. Hrg. 107-852, Serial No. J-107-60); *Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 1st Sess. (Nov. 14, 2001) (S. Hrg. 107-657, Serial No. J-107-46A); *Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106th Cong., 2nd Sess. (July 12, 2000) (S. Hrg. 106-902, Serial No. J-106-97); *ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106th Cong., 2nd Sess. (Mar. 7, 2000) (S. Hrg. 106-885, Serial No. J-106-70); *The Identity Theft and Assumption Deterrence Act: S. 512: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 105th Cong., 2nd Sess. (May 20, 1998) (S. Hrg. 105-845, Serial No. J-105-104).

²⁹⁴ See Identity Theft Penalty Enhancement Act, 18 U.S.C. § 1028A (2004); Social Security Number Confidentiality Act of 2000, 31 U.S.C. § 3327 (2000); Internet False Identification Prevention Act of 2000, 18 U.S.C §§ 1001, 1028 (2000); Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C § 1028 (1998).

²⁹⁵ Press Release, The White House, Remarks by the President at Signing of Identity Theft Penalty Enhancement Act (July 15, 2004), <http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html>.

Information Officer and Associate Vice Chancellor for Information Technology, University of California, Los Angeles; (2) Joanne McNabb, Director, California Office of Privacy Protection; and (3) Chris Jay Hoofnagle, Staff Attorney and Senior Fellow, Berkeley Center for Law and Technology, University of California, Berkeley.

Identity Theft: A Growing Problem

At the hearing, Senator Feinstein explained the magnitude of the threat from data breaches: “Since the beginning of 2005 . . . over 100 million data records containing individuals’ most sensitive personal financial data, health data, other kinds of data, have been exposed due to data breaches.”²⁹⁶ Senator Kyl described the extent of the identity theft problem: “[I]dentity-theft related crime cost business and individuals . . . nearly \$50 billion in 2006, and an estimated 8.4 million Americans were victims of ID theft in 2006, about 1 in 25 people.”²⁹⁷

Causes of Identity Theft

As the President’s Identity Theft Task Force put it, “[identity theft] is a problem with no single cause and no single solution.”²⁹⁸ Senator Kyl explained that methamphetamine use, illegal immigration, and terrorism contribute to the problem,²⁹⁹ and Ms. Parnes added that “the failure to protect consumers’ sensitive personal information, which can lead to data breaches; and the availability of [Social Security numbers], with which identity thieves can open new accounts in consumers’ names” has also contributed to the identity theft problem.³⁰⁰

Data Breaches

In 2005 and 2006, the security of over 100 million data records containing sensitive, personal data were compromised due to data breaches.³⁰¹ Data breaches can

²⁹⁶ Hearing of Mar. 21, 2007, at 2 (statement of Dianne Feinstein).

²⁹⁷ Hearing of Mar. 21, 2007, at 3 (statement of Jon Kyl).

²⁹⁸ President’s Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan 1* (Apr. 2007), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

²⁹⁹ Hearing of Mar. 21, 2007, at 4 (statement of Jon Kyl).

³⁰⁰ Hearing of Mar. 21, 2007, at 3 (written statement of Lydia Parnes).

³⁰¹ Hearing of Mar. 21, 2007, at 2 (statement of Dianne Feinstein).

harm individuals, cause vast economic losses, and stifle commerce.³⁰² “Although not all data breaches result in identity theft, some do. And for that reason it is critical that those who maintain sensitive consumer information adequately protect it.”³⁰³

Data Breach Notification

Consumers should be notified in the event that their personal data are compromised. For example, identity theft laws, such as credit freezes, only work if individuals know that they are potential victims.³⁰⁴

According to Ms. McNabb, California’s data breach law³⁰⁵ “has served as a stimulus to organizations to improve their practices for handling personal information . . .”³⁰⁶ Mr. Hoofnagle agreed: “Breach notification has caused a serious increase in investment in security. Prior to the passage of [breach] laws, companies could simply not disclose security breaches and let consumers bear the costs of identity theft and other harms.”³⁰⁷

Data breach notification laws must strike a careful balance. As Senator Feinstein explained:

If notices are sent even when a breach poses no risk of harm, consumers tune it out. Yet if notices are only sent when there is a high likelihood of harm, notices will not be sent often enough because in many cases it will be hard to predict whether the data will be used for identity theft.³⁰⁸

Accordingly, data breach laws should contain a “risk of harm” standard to ensure that notification is only required when warranted.³⁰⁹ Mr. Davis agreed that such a standard is a “good principle,” but he also noted that a standard such as “significant

³⁰² Hearing of Mar. 21, 2007, at 2 (statement of Dianne Feinstein).

³⁰³ Hearing of Mar. 21, 2007, at 7 (statement of Lydia Parnes).

³⁰⁴ Hearing of Mar. 21, 2007, at 2 (statement of Dianne Feinstein).

³⁰⁵ Hearing of Mar. 21, 2007, at 23 (statement of Joanne McNabb).

³⁰⁶ Hearing of Mar. 21, 2007, at 18 (statement of Joanne McNabb).

³⁰⁷ Hearing of Mar. 21, 2007, at 20 (statement of Chris Hoofnagle).

³⁰⁸ Hearing of Mar. 21, 2007, at 11 (statement of Dianne Feinstein).

³⁰⁹ Hearing of Mar. 21, 2007, at 21 (statement of Dianne Feinstein).

risk of harm” could result in a notification for nearly every data breach that occurs because of the difficulty of defining what constitutes “significant risk” and “harm.”³¹⁰

California’s breach notification law requires notification when “data is acquired by an unauthorized person,”³¹¹ and according to Ms. McNabb, the law “has served as a stimulus to organizations to improve their practices for handling personal information . . .”³¹² Mr. Hoofnagle agreed: “Breach notification has caused a serious increase in investment in security. Prior to the passage of [breach] laws, companies could simply not disclose security breaches and let consumers bear the costs of identity theft and other harms.”³¹³ He suggested that breach notification laws should require “standardized, central, and public reporting of breaches . . .”³¹⁴ Mr. Tenpas noted, however, that data breach laws requiring federal agencies to provide notice would be premature because agencies should be given time to implement the President’s Identity Theft Task Force interim recommendations.³¹⁵

The Federal Government’s Efforts to Combat Identity Theft

The Department of Justice (DOJ) works with various federal agencies, including the Federal Bureau of Investigation, the U.S. Postal Inspection Service, the Secret Service, and the Social Security Administration, to investigate and prosecute identity thieves.³¹⁶ In its prosecution of identity thieves, DOJ relies heavily on the criminal sentencing requirements set forth in the Identity Theft Penalty Enhancement Act,³¹⁷ which Senators Feinstein and Kyl sponsored.³¹⁸ Since the enactment of the Identity Theft Penalty Enhancement Act, federal prosecutions of identity thieves have increased dramatically. In 2006, 507 defendants were charged with identity theft, up from 226 defendants in 2005.³¹⁹ DOJ investigates and prosecutes many different types of identity

³¹⁰ Hearing of Mar. 21, 2007, at 22 (statement of Jim Davis).

³¹¹ Hearing of Mar. 21, 2007, at 23 (statement of Joanne McNabb).

³¹² Hearing of Mar. 21, 2007, at 18 (statement of Joanne McNabb).

³¹³ Hearing of Mar. 21, 2007, at 20 (statement of Chris Hoofnagle).

³¹⁴ Hearing of Mar. 21, 2007, at 20 (statement of Chris Hoofnagle).

³¹⁵ Hearing of Mar. 21, 2007, at 11 (statement of Ronald Tenpas).

³¹⁶ Hearing of Mar. 21, 2007, at 1 (written statement of Ronald Tenpas).

³¹⁷ Hearing of Mar. 21, 2007, at 1 (written statement of Ronald Tenpas).

³¹⁸ Identity Theft Penalty Enhancement Act, 18 U.S.C. § 1028A (2004).

³¹⁹ Hearing of Mar. 21, 2007, at 1 (written statement of Ronald Tenpas).

theft cases, including cases involving organized crime, Internet-based international fraud schemes, health-care fraud, and the theft of patient information.³²⁰

The Federal Trade Commission (FTC) combats identity theft by “educating businesses about data security and enforcing the existing Federal data security laws.”³²¹ In March 2007, the FTC issued a guide that provides businesses with “comprehensive advice on developing and implementing reasonable data security procedures.”³²² Since 2001, the FTC has filed 14 cases against companies to “challeng[e] inadequate data security practices.”³²³ The FTC also maintains an identity theft website and hotline where it receives nearly 20,000 contacts each week;³²⁴ in 2006, it received roughly 250,000 complaints of identity theft from consumers.³²⁵

President’s Identity Theft Task Force

On May 10, 2006, President Bush issued an executive order that established the President’s Identity Theft Task Force (Task Force).³²⁶ The Task Force is chaired by both the Attorney General and the chairman of the FTC, and membership consists of representatives from 15 other federal departments and agencies.³²⁷ The purpose of the Task Force is “to use Federal resources effectively to deter, prevent, detect, investigate, proceed against, and prosecute” identity thieves.³²⁸

³²⁰ Hearing of Mar. 21, 2007, at 2-4 (written statement of Ronald Tenpas).

³²¹ Hearing of Mar. 21, 2007, at 8 (statement of Lydia Parnes).

³²² Hearing of Mar. 21, 2007, at 8 (statement of Lydia Parnes).

³²³ Hearing of Mar. 21, 2007, at 8 (statement of Lydia Parnes).

³²⁴ Hearing of Mar. 21, 2007, at 9 (statement of Lydia Parnes).

³²⁵ Hearing of Mar. 21, 2007, at 2 (statement of Dianne Feinstein).

³²⁶ Strengthening Federal Efforts to Protect Against Identity Theft, Exec. Order No. 13,402, 71 C.F.R. 27,945 (May 10, 2006), available at <http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html>.

³²⁷ Hearing of Mar. 21, 2007, at 6 (statement of Ronald Tenpas); President’s Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (Apr. 2007), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf> (The President’s Identity Theft Task Force is composed of representatives from Department of Justice, Federal Trade Commission, Department of Treasury, Department of Commerce, Department of Health and Human Services, Department of Veterans Affairs, Department of Homeland Security, Office of Management and Budget, United States Postal Service, Federal Reserve System, Office of Personnel Management, Federal Deposit Insurance Corporation, Securities and Exchange Commission, National Credit Union Administration, Social Security Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision).

³²⁸ Strengthening Federal Efforts to Protect Against Identity Theft, Exec. Order No. 13,402, 71 C.F.R. 27,945 (May 10, 2006), available at <http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html>.

The Task Force released an interim report in September 2006 that contained seven interim recommendations.³²⁹ These recommendations focused on three areas: (1) improving the government's maintenance of personal data; (2) providing restitution for identity theft victims; and (3) authorizing the creation of a universal police report.³³⁰ The Task Force worked with federal agencies to implement these recommendations³³¹ and released its final report in April 2007.³³² The final report reiterated the previously released interim recommendations and offered new recommendations for establishing national data breach notification procedures.³³³

State Identity Theft Laws and Solutions

States have been leading the fight against identity thieves. California, in particular, has been at the forefront of identity theft legislation, having passed more than 80 privacy laws since 1999,³³⁴ many of which have been subsequently replicated in other states.³³⁵ For example, California was the first state in the nation to enact credit freeze legislation.³³⁶ Credit freezes prevent credit bureaus from releasing consumers' credit reports without permission, which makes it much more difficult for accounts to be fraudulently opened.³³⁷ Over 25 states have enacted credit freeze laws, and more than a dozen states are considering credit freeze legislation.³³⁸

³²⁹ President's Identity Theft Task Force, *Summary of Interim Recommendations 1* (Sept. 2006), available at <http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf>.

³³⁰ President's Identity Theft Task Force, *Summary of Interim Recommendations 1* (Sept. 2006), available at <http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf>.

³³¹ Hearing of Mar. 21, 2007, at 6 (statement of Ronald Tenpas).

³³² President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (Apr. 2007), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

³³³ President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* 35 (Apr. 2007), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

³³⁴ Hearing of Mar. 21, 2007, at 18 (statement of Joanne McNabb).

³³⁵ Hearing of Mar. 21, 2007, at 18 (statement of Joanne McNabb).

³³⁶ Hearing of Mar. 21, 2007, at 18 (statement of Joanne McNabb); Steve Jordan, *Plans' Goal: Stop ID Theft Cold*, OMAHA WORLD-HERALD, Mar. 3, 2007, at 01D.

³³⁷ Paul Davenport, *Lawmakers Move to Let Arizonans Freeze Credit Reports*, ARIZ. CAPITOL TIMES, Feb. 16, 2007.

³³⁸ Steve Jordan, *Plans' Goal: Stop ID Theft Cold*, OMAHA WORLD-HERALD, Mar. 3, 2007, at 01D.

Notification of Risk to Personal Data Act (S. 239)

Senator Feinstein introduced S. 239, the Notification of Risk to Personal Data Act (Act), in January 2007.³³⁹ The Act would require any agency or business entity involved with sensitive, personally identifiable information to notify individuals affected by a breach without unreasonable delay, unless it is determined that no “significant risk of harm” resulted from the breach.³⁴⁰ Notifications must include a description of the compromised information, a toll-free contact number for the agency or business, and contact information for all major credit reporting agencies.³⁴¹ The Act would also provide a notification exemption for national security and law enforcement purposes,³⁴² and would authorize the Attorney General or state attorneys general to bring civil and injunctive actions against any business entity suspected of violating breach notification rules.³⁴³

Conclusion

Senators Feinstein and Kyl recognize that “[t]here is no quick solution to [the identity theft] problem.”³⁴⁴ There are, however, many steps that can be taken to reduce the frequency and severity of this growing problem. For instance, Lydia Parnes testified that governments and businesses must do more to “improve authentication of identities” and to prevent identity thieves from opening new accounts with stolen information.³⁴⁵ She also recommended that consumers and businesses be educated about identity theft, so that they can better protect themselves³⁴⁶ and their customers’ sensitive account information.³⁴⁷

The Subcommittee is also supportive of the many actions taken by the Executive in recent years to address this growing problem. For instance, at the time of the

³³⁹ Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007).

³⁴⁰ Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. § 2 (2007).

³⁴¹ Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. § 5 (2007).

³⁴² Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. §§ 2-3 (2007).

³⁴³ Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. §§ 7-8 (2007).

³⁴⁴ President’s Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan IX* (Apr. 2007), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

³⁴⁵ Hearing of Mar. 21, 2007, at 8 (statement of Lydia Parnes).

³⁴⁶ Hearing of Mar. 21, 2007, at 8 (statement of Lydia Parnes).

³⁴⁷ Hearing of Mar. 21, 2007, at 12-13 (statement of Lydia Parnes).

hearing, the Department of Justice was actively prosecuting identity theft cases, while the Federal Trade Commission focused on better informing consumers and businesses about identity theft prevention.³⁴⁸ In May 2006, President Bush also established the President's Identity Theft Task Force "to use Federal resources effectively to deter, prevent, detect, investigate, proceed against, and prosecute" identity theft.³⁴⁹ Finally, within Congress, Senators Feinstein and Kyl acted to address the issue of data breaches, a form of large-scale identity theft that can harm individuals, create economic losses, and stifle commerce.³⁵⁰ Senator Feinstein introduced S. 239, the Notification of Risk to Personal Data Act,³⁵¹ which would create a federal data breach notification law, and Senator Kyl cosponsored similar legislation, S. 2102, the Personal Data Protection Act.³⁵² While neither bill received a vote during the 110th Congress, Senators Feinstein and Kyl remain committed to protecting personally identifiable information, and will continue to work with their Senate colleagues to develop new strategies for preventing identity theft.

The Legal Rights of Guantanamo Detainees: What Are They, Should They Be Changed, and Is an End in Sight?

Introduction

On December 11, 2007, the Subcommittee held a hearing entitled "The Legal Rights of Guantanamo Detainees: What Are They, Should They Be Changed, and Is an End in Sight?" to inquire whether holding alien enemy combatants at Guantanamo Bay is in the best interests of our country.

Five experts testified at the hearing: (1) Brigadier General Thomas Hartmann, Legal Advisor to the Convening Authority, Office of Military Commissions; (2) Steven Engel, Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice; (3) Mark Denbeaux, Professor of Law, Seton Hall Law School; (4) Navy Rear

³⁴⁸ Hearing of Mar. 21, 2007, at 1 (written statement of Ronald Tenpas); *id.* at 7-8 (statement of Lydia Parnes).

³⁴⁹ Strengthening Federal Efforts to Protect Against Identity Theft, Exec. Order No. 13,402, 71 C.F.R. 27,945 (May 10, 2006), *available at* <http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html>.

³⁵⁰ Hearing of Mar. 21, 2007, at 1-2 (statement of Dianne Feinstein).

³⁵¹ Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. §§ 2-3, 7 (2007).

³⁵² Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007).

Admiral John Hutson; and (5) Debra Burlingame, Member of the Board of Directors, National September 11 Memorial Foundation.

Background

The United States government established a detention center at Guantanamo Bay Naval Base in southeastern Cuba to hold suspected terrorists and enemy combatants. The first detainees arrived in January 2002. Because Guantanamo Bay is not part of the territorial United States, there was uncertainty about which legal strictures applied to the detention center.

On June 28, 2004, the Supreme Court held in *Hamdi v. Rumsfeld*³⁵³ that Congress' 2001 Authorization for Use of Military Force (AUMF) authorized the President to detain individuals who fought against the United States in Afghanistan, regardless of whether they were American citizens, and that such detention was only authorized until the end of hostilities. The Court also held that citizen-detainees had to receive notice of the factual basis for their classification as an enemy combatant, and a fair opportunity to rebut the Government's factual assertions before a neutral decisionmaker.³⁵⁴ The next day, on June 29, 2004, the Supreme Court ruled in *Rasul v. Bush*³⁵⁵ that federal courts have the jurisdiction to consider the habeas corpus petitions of non-citizen detainees held at Guantanamo Bay. After this ruling, all detainees were granted a combatant status review tribunal (CSRT hearing) to evaluate whether they were properly classified as enemy combatants.³⁵⁶ A limited number of detainees were to be tried by military commissions.

In *Hamdan v. Rumsfeld*,³⁵⁷ the Supreme Court struck down the procedures of these commissions because they violated the Uniform Code of Military Justice (UMCJ) and the Geneva Conventions (GC) and were not based on statute. In response to the *Hamdan* decision, the Military Commissions Act (S. 3930) was introduced. The

³⁵³ *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004).

³⁵⁴ *Hamdi v. Rumsfeld*, 542 U.S. 507, 509 (2004).

³⁵⁵ *Rasul v. Bush*, 542 U.S. 466 (2004).

³⁵⁶ *The Legal Rights of Guantanamo Detainees: What Are They, Should They Be Changed, and Is an End in Sight?: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 1st Sess. (Dec. 11, 2007) (S. Hrg. 110-____, Serial No. J-110-____), at 3 (transcript) (statement of Dianne Feinstein) [hereinafter "Hearing of Dec. 11, 2007"].

³⁵⁷ *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006).

Military Commissions Act passed by a 65 to 34 bipartisan vote and was signed into law by President Bush in October 2006.³⁵⁸ The Act sought to establish procedures and standards for the fair treatment and trial of alien enemy combatants captured in the war against terrorists. It was intended to meet the requirements of the Supreme Court's ruling in the *Hamdan* decision and fulfill United States government obligations under Common Article 3 of the Geneva Convention.

In *Boumediene v. Bush*, the Supreme Court held that federal habeas corpus rights extended to detainees held at Guantanamo, and that the Military Commissions Act of 2006 was an unconstitutional deprivation of the right of habeas corpus.³⁵⁹

The History of Releasing Guantanamo Detainees

During discussion about releasing detainees from Guantanamo, Senator Feinstein explained that of the 759 detainees brought to Guantanamo since January 2002, some 454 had been released or had died, and 305 remained detained at the detention center.³⁶⁰ However, of the remaining 305 detainees, only four detainees had been officially charged with any crime and none had been tried by any court or military commission.³⁶¹ Senator Kyl pointed out that, of those detainees released from Guantanamo Bay, Department of Defense (DOD) figures account for at least 30 detainees who returned to wage war against the United States and its allies.³⁶² A dozen released detainees were killed in battle by U.S. forces, while others were recaptured.³⁶³ Two released detainees later became regional commanders for Taliban forces. Another attacked United States and allied soldiers in Afghanistan, killing three Afghan soldiers. Yet another killed an Afghan judge and one led a terrorist attack on a Pakistani hotel that led to a kidnapping raid and the death of a Chinese civilian.³⁶⁴

Mr. Denbeaux, Professor of Law at Seton Hall Law School, reviewed publicly released DOD information and concluded that the military only charged 45 percent of the detainees in Guantanamo with ever having committed any hostile act against the

³⁵⁸ Military Commissions Act of 2006, Pub. L. No. 109-366, 120 Stat. 2601 (2006).

³⁵⁹ *Boumediene v. Bush*, 128 S. Ct. 2229, 2240 (2008).

³⁶⁰ Hearing of Dec. 11, 2007, at 2 (transcript) (statement of Dianne Feinstein).

³⁶¹ Hearing of Dec. 11, 2007, at 2 (transcript) (statement of Dianne Feinstein); *id.* at 4

³⁶² Hearing of Dec. 11, 2007, at 8 (transcript) (statement of Jon Kyl).

³⁶³ Hearing of Dec. 11, 2007, at 8 (transcript) (statement of Jon Kyl).

³⁶⁴ Hearing of Dec. 11, 2007, at 8 (transcript) (statement of Jon Kyl).

United States or coalition forces.³⁶⁵ He testified that only 21 of the 759 detainees were ever on the battlefield, and that as of 2004 only 24 of those detained at Guantanamo were captured by United States forces.³⁶⁶ Senator Durbin pointed out that, based on Professor Denbeaux's numbers, it would not impose too great a burden on the government to require troops to testify at military commissions against these 21 detainees, rather than to allow hearsay.³⁶⁷

Steven Engel, a Deputy Assistant Attorney General in the Office of Legal Counsel at the Department of Justice, countered Professor Denbeaux's testimony by asserting that upwards of 30 former detainees had returned to various theaters to wage jihad against American or allied forces.³⁶⁸ Mr. Engel also testified that these DOD numbers were only reflective of what the DOD released publicly.³⁶⁹ He added that at the time of the hearing, about 759 detainees had been brought to Guantanamo, approximately 455 had been released, and the remaining 305 were still there.³⁷⁰

The Authority of Military Law During Wartime

Senator Graham argued that because our enemy is composed of non-uniformed soldiers who are at war with us, we have the obligation to follow the law of armed conflict when we capture one of them.³⁷¹ He added that once combatants are captured and their status is to be determined, that decision should be made by the military, not a federal judge.³⁷² Senator Graham also noted that Article 5 of the Geneva Convention requires a competent tribunal to decide whether or not someone is an unlawful enemy combatant, a traditional prisoner of war, or an innocent civilian.³⁷³

³⁶⁵ Hearing of Dec. 11, 2007, at 74 (transcript) (statement of Mark Denbeaux).

³⁶⁶ Hearing of Dec. 11, 2007, at 74 (transcript) (statement of Mark Denbeaux); it is important to note that Denbeaux's conclusions do not account for classified evidence relating to the detainees.

³⁶⁷ Hearing of Dec. 11, 2007, at 57-58 (transcript) (statement of Richard Durbin).

³⁶⁸ Hearing of Dec. 11, 2007, at 32 (transcript) (statement of Jon Kyl).

³⁶⁹ Hearing of Dec. 11, 2007, at 33 (transcript) (statement of Steven Engel).

³⁷⁰ Hearing of Dec. 11, 2007, at 34 (transcript) (statement of Steven Engel).

³⁷¹ Hearing of Dec. 11, 2007, at 63 (transcript) (statement of Lindsey Graham).

³⁷² Hearing of Dec. 11, 2007, at 64 (transcript) (statement of Lindsey Graham).

³⁷³ Hearing of Dec. 11, 2007, at 64 (transcript) (statement of Lindsey Graham).

Senator Graham described the factors used to determine whether to release a detainee.³⁷⁴ First, is there any new evidence that could change a detainee's status?³⁷⁵ Second, does the detainee have intelligence value that would be useful to the U.S. government?³⁷⁶ And lastly, is the detainee still a threat?³⁷⁷ He added that a review board meets annually to determine whether detainee status has changed, and over 400 detainees were released through that process at the time of this hearing.³⁷⁸

Characteristics of the Military Commissions Act

Under the Military Commissions Act, terrorist detainees are provided access to all evidence against them, unless disclosure of that evidence would be detrimental to U.S. national security.³⁷⁹ If the national security privilege is invoked, the military judge must, to the extent possible, provide the detainee with an appropriate substitute that conveys relevant information while avoiding the disclosure of classified information.³⁸⁰ The legislation also sought to protect sources and methods of gathering confidential information.³⁸¹

Brigadier General Hartmann, the Legal Advisor to the Convening Authority of the Department of Defense Office of Military Commissions, described how the military attempted to ensure a fair trial for detainees, including appointing military and civilian defense counsel.³⁸² He noted that U.N. observers, members of the press, and members of different non-governmental organizations (NGOs) attend the hearings.³⁸³ In one case, the accused was allowed to seek witnesses that were exculpatory, and the convening authority even granted immunity to a witness so that the evidence could be given.³⁸⁴ If found guilty, an accused detainee has a right that no other person in the United States has in any other court: the right to appeal to the Court of Military

³⁷⁴ Hearing of Dec. 11, 2007, at 65 (transcript) (statement of Lindsey Graham).

³⁷⁵ Hearing of Dec. 11, 2007, at 65 (transcript) (statement of Lindsey Graham).

³⁷⁶ Hearing of Dec. 11, 2007, at 65 (transcript) (statement of Lindsey Graham).

³⁷⁷ Hearing of Dec. 11, 2007, at 65 (transcript) (statement of Lindsey Graham).

³⁷⁸ Hearing of Dec. 11, 2007, at 65 (transcript) (statement of Lindsey Graham).

³⁷⁹ Military Commissions Act of 2006, Pub. L. No. 109-366, § 949a, 120 Stat. 2601, 2608 (2006).

³⁸⁰ Military Commissions Act of 2006, Pub. L. No. 109-366, § 949d, 120 Stat. 2601, 2612 (2006).

³⁸¹ Military Commissions Act of 2006, Pub. L. No. 109-366, § 949d, 120 Stat. 2601, 2612 (2006).

³⁸² Hearing of Dec. 11, 2007, at 17 (transcript) (statement of Thomas Hartmann).

³⁸³ Hearing of Dec. 11, 2007, at 17 (transcript) (statement of Thomas Hartmann).

³⁸⁴ Hearing of Dec. 11, 2007, at 18 (transcript) (statement of Thomas Hartmann).

Commission Review.³⁸⁵ The accused would also have the right to have his sentence reviewed by the convening authority, which could only reduce the sentence, not increase it.³⁸⁶ General Hartmann added that this is a right that only exists in the Uniform Code of Military Justice.³⁸⁷

Senator Feinstein asked General Hartmann whether he thought that military commission trials should be open and whether information obtained from coercive interrogation techniques, like waterboarding, would be used in military commissions and whether such information was reliable.³⁸⁸ General Hartmann repeated that there are often press and NGOs at these trials except for when classified evidence is used, but declined to state whether evidence obtained from coercive interrogation was being used in military commissions because of the pendency of the cases at Guantanamo. General Hartmann also testified that evidence would be used in accordance with applicable rules of evidence.³⁸⁹ General Hartmann reminded the Subcommittee of the open nature of detainee trials at Guantanamo: “Let me make one clarification, which often gets in the newspaper, which is inaccurate and that refers to the word ‘secret’ trials. There will be no secret trials. There is no mechanism for a secret trial.”³⁹⁰ Senator Durbin took issue with General Hartmann’s characterization that the military commissions are transparent.³⁹¹ As an example, Senator Durbin noted that in the case of Omar Khadir, defense lawyers were ordered not to disclose to Mr. Khadir, or anyone else, who would appear as a witness against the defendant.³⁹² General Hartmann explained that 21 days before a trial, the prosecution has the burden of explaining why the identities of witnesses must be withheld.³⁹³ If the prosecution fails to do so, then all witnesses are made available to defense counsel and the accused.³⁹⁴ Senator Cardin expressed his desire for a public discussion of the process by which the government evaluates the quality of the evidence it uses to prosecute the detainees.³⁹⁵ General Hartmann

³⁸⁵ Hearing of Dec. 11, 2007, at 18-19 (transcript) (statement of Thomas Hartmann).

³⁸⁶ Hearing of Dec. 11, 2007, at 14 (transcript) (statement of Thomas Hartmann).

³⁸⁷ Hearing of Dec. 11, 2007, at 19 (transcript) (statement of Thomas Hartmann).

³⁸⁸ Hearing of Dec. 11, 2007, at 29 (transcript) (statement of Dianne Feinstein).

³⁸⁹ Hearing of Dec. 11, 2007, at 29 (transcript) (statement of Thomas Hartmann).

³⁹⁰ Hearing of Dec. 11, 2007, at 29 (transcript) (statement of Thomas Hartmann).

³⁹¹ Hearing of Dec. 11, 2007, at 54 (transcript) (statement of Richard Durbin).

³⁹² Hearing of Dec. 11, 2007, at 54 (transcript) (statement of Richard Durbin).

³⁹³ Hearing of Dec. 11, 2007, at 54 (transcript) (statement of Thomas Hartmann).

³⁹⁴ Hearing of Dec. 11, 2007, at 54 (transcript) (statement of Thomas Hartmann).

³⁹⁵ Hearing of Dec. 11, 2007, at 42 (transcript) (statement of Benjamin Cardin).

responded that the rules of evidence determined these procedures.³⁹⁶ He went on to explain that once the prosecutor tries to use evidence in court, the American system allows the defense counsel to challenge that evidence.³⁹⁷ At that point a military judge will evaluate it, and the world press can report on the decision and the process.³⁹⁸

Habeas Corpus Rights for Detainees

The members of the Subcommittee reached different conclusions regarding habeas corpus rights for detainees. Senators Feinstein and Cardin expressed their desire to confer these rights. Senator Cardin explained that, because the United States failed to engage with the international community in setting up procedures for handling detainees, and is unilaterally determining who is sent to Guantanamo Bay, a robust and transparent judicial proceeding is essential in order to ensure those who are at Guantanamo Bay belong there.³⁹⁹ Senators Kyl, Sessions, and Graham warned of the problems such a course would entail. Senator Kyl noted that habeas rights for enemy combatant detainees are “problematic, among other things, because detainees will demand access to classified evidence.”⁴⁰⁰ This could jeopardize the anonymity of American intelligence sources and relations with some Middle Eastern governments, whom are among our most sensitive sources of information on Al Qaida.⁴⁰¹

While Mr. Engel noted that the Constitution allows temporary suspension of the writ of habeas corpus,⁴⁰² he posited questions about the possible implications of granting habeas corpus rights to detainees at Guantanamo: Would detainees have to be brought to the U.S. for habeas hearings?⁴⁰³ What rules of discovery would govern such proceedings?⁴⁰⁴ Could the detainees compel a U.S. soldier to return from Afghanistan or Iraq in order to appear and testify at such a hearing?⁴⁰⁵ Mr. Engel did not think that these questions would need to be answered because he believed the Detainee Treatment

³⁹⁶ Hearing of Dec. 11, 2007, at 42 (transcript) (statement of Thomas Hartmann).

³⁹⁷ Hearing of Dec. 11, 2007, at 44 (transcript) (statement of Thomas Hartmann).

³⁹⁸ Hearing of Dec. 11, 2007, at 44 (transcript) (statement of Thomas Hartmann).

³⁹⁹ Hearing of Dec. 11, 2007, at 39 (transcript) (statement of Benjamin Cardin).

⁴⁰⁰ Hearing of Dec. 11, 2007, at 9 (transcript) (statement of Jon Kyl).

⁴⁰¹ Hearing of Dec. 11, 2007, at 10 (transcript) (statement of Jon Kyl).

⁴⁰² Hearing of Dec. 11, 2007, at 22 (transcript) (statement of Steven Engel).

⁴⁰³ Hearing of Dec. 11, 2007, at 24 (transcript) (statement of Steven Engel).

⁴⁰⁴ Hearing of Dec. 11, 2007, at 24 (transcript) (statement of Steven Engel).

⁴⁰⁵ Hearing of Dec. 11, 2007, at 24 (transcript) (statement of Steven Engel).

Act procedures themselves provided a robust process that would be a constitutionally adequate.⁴⁰⁶

Characteristics of the Detainee Treatment Act

Mr. Engel testified that while the Detainee Treatment Act did restrict the availability of habeas corpus to the detainees, it still gave them a day in court.⁴⁰⁷ Mr. Engel said that the Act holds that detainees, after receiving fair hearings before the combat status review tribunals (CSRT) of the Department of Defense, can seek review of those decisions at the D.C. Circuit Court.⁴⁰⁸ Mr. Engel asserted that the CSRT procedures go beyond the requirements of the Geneva Conventions and the requirements owed to lawful prisoners of war, and that they provide the due process which the Supreme Court, in *Hamdan*, held appropriate for American citizens who choose to fight for the enemy and are subsequently detained.⁴⁰⁹ The right of a detainee to have a CSRT decision reviewed by the D.C. Circuit Court, said Engel, is virtually unprecedented during wartime.⁴¹⁰

No Precedent for Extending Habeas Corpus Rights to Detainees

Senator Kyl questioned the premise that extending habeas corpus rights to detainees was a matter of principle and noted that if this were true, it should have been applied in past wars.⁴¹¹ He also noted that we are holding thousands of detainees in Afghanistan and Iraq and that if the detainees at Guantanamo Bay could sue the United States government, then there is no reason that the thousands of detainees at our international military bases could not also sue;⁴¹² after all, the United States military's control over Guantanamo is no greater than its control over any other military base in the world.⁴¹³ Senator Kyl added that "[a]t the very least, we should be able to agree that

⁴⁰⁶ Hearing of Dec. 11, 2007, at 24 (transcript) (statement of Steven Engel).

⁴⁰⁷ Hearing of Dec. 11, 2007, at 22 (transcript) (statement of Steven Engel).

⁴⁰⁸ Hearing of Dec. 11, 2007, at 22 (transcript) (statement of Steven Engel).

⁴⁰⁹ Hearing of Dec. 11, 2007, at 23 (transcript) (statement of Steven Engel).

⁴¹⁰ Hearing of Dec. 11, 2007, at 23 (transcript) (statement of Steven Engel).

⁴¹¹ Hearing of Dec. 11, 2007, at 11 (transcript) (statement of Jon Kyl).

⁴¹² Hearing of Dec. 11, 2007, at 11 (transcript) (statement of Jon Kyl).

⁴¹³ Hearing of Dec. 11, 2007, at 11 (transcript) (statement of Jon Kyl).

we should not extend greater rights and privileges to combatants who violate the [laws] of war, including terrorists, than we do to those who obey the laws of war.”⁴¹⁴

Senator Sessions supported the legal framework in place at Guantanamo. “When you say [detainees] should be brought to justice, if that means captured prisoners of war have to be tried, then I don’t agree. Prisoners of war are not tried. They are detained until hostilities end.”⁴¹⁵ He added that we cannot transform military detention of unlawful combatants, who do not comply with the rules of war, into trials.⁴¹⁶ Senator Sessions pointed out that in the history of Anglo-American jurisprudence, habeas corpus relief has never been granted to a detainee during wartime.⁴¹⁷

Senator Cardin, on the other hand, concluded that the detainees are essentially criminals and are entitled to habeas rights.⁴¹⁸ As he pointed out, to hold them as prisoners of war, without basic rights, is dangerous because the war on terror is unlikely to have a definitive end.⁴¹⁹ Senators Feinstein, Cardin, and Durbin all pointed out that the uncertain nature of Guantanamo Bay, and the uncertainty of the legal status of the detainees within, was hurting the standing of the United States abroad.⁴²⁰ Quoting former Secretary of State Colin Powell, Senator Durbin reiterated that Guantanamo Bay has “shaken the belief the world had in America’s justice system . . . and it’s causing us far more damage any good we get for it.”⁴²¹

Negative Effects of Habeas-Type Litigation on Interrogation of Detainees

Mr. Engel discussed the effect that the initial *Rasul* decision, which allowed statutory habeas jurisdiction, had on interrogation of Al Qaeda detainees held at Guantanamo.⁴²² He said that lawyers for the detainees had boasted that any kind of

⁴¹⁴ Hearing of Dec. 11, 2007, at 11 (transcript) (statement of Jon Kyl).

⁴¹⁵ Hearing of Dec. 11, 2007, at 14 (transcript) (statement of Jeff Sessions).

⁴¹⁶ Hearing of Dec. 11, 2007, at 14 (transcript) (statement of Jeff Sessions).

⁴¹⁷ Hearing of Dec. 11, 2007, at 50-51 (transcript) (statement of Jeff Sessions).

⁴¹⁸ Hearing of Dec. 11, 2007, at 40 (transcript) (statement of Benjamin Cardin).

⁴¹⁹ Hearing of Dec. 11, 2007, at 40 (transcript) (statement of Benjamin Cardin).

⁴²⁰ Hearing of Dec. 11, 2007, at 3 (transcript) (statement of Dianne Feinstein); hearing of Dec. 11, 2007, at 13 (transcript) (statement of Benjamin Cardin); hearing of Dec. 11, 2007, at 61 (transcript) (statement of Richard Durbin).

⁴²¹ Hearing of Dec. 11, 2007, at 60 (transcript) (statement of Richard Durbin).

⁴²² Hearing of Dec. 11, 2007, at 35 (transcript) (statement of Jon Kyl).

effective interrogation is impossible once the detainee has regular access to a lawyer.⁴²³ The key to effective interrogation, he explained, is the rapport between the interrogator and the subject,⁴²⁴ and any good attorney representing a detainee would be able to shut down that rapport immediately.⁴²⁵ Senator Sessions echoed the concern that the unprecedented use of defense lawyers is harming the prosecution's ability to meaningfully interrogate the detainees.⁴²⁶

Mr. Engel explained that the current war against terrorists is unlike any in our history because our enemies show no respect for the law of war, do not wear uniforms, and seek to achieve their goals through covert attacks on civilians rather than our armed forces.⁴²⁷ He pointed out that while our commitment to the rule of law is our strength, it has to be reconciled with the need to prosecute this armed conflict and protect the nation against further attacks.⁴²⁸

Characteristics of the Detainee Treatment Act

Mr. Engel explained that while the Detainee Treatment Act did restrict the availability of habeas corpus to the detainees, it still gave them a day in court.⁴²⁹ The Act holds that detainees, after receiving fair hearings before the combat status review tribunals (CSRT) of the Department of Defense, can seek review of those decisions at the D.C. Circuit Court.⁴³⁰ These CSRT procedures go beyond the requirements of the Geneva Convention, the requirements owed to lawful prisoners of war, and also the provisions for due process that the Supreme Court, in *Hamdan*, held appropriate for American citizens who choose to fight for the enemy and are subsequently detained.⁴³¹ The right of a detainee to have a CSRT decision reviewed by the D.C. Circuit Court is virtually unprecedented during wartime.⁴³²

⁴²³ Hearing of Dec. 11, 2007, at 35-36 (transcript) (statement of Steven Engel).

⁴²⁴ Hearing of Dec. 11, 2007, at 36 (transcript) (statement of Steven Engel).

⁴²⁵ Hearing of Dec. 11, 2007, at 36 (transcript) (statement of Steven Engel).

⁴²⁶ Hearing of Dec. 11, 2007, at 51 (transcript) (statement of Jeff Sessions).

⁴²⁷ Hearing of Dec. 11, 2007, at 21 (transcript) (statement of Steven Engel).

⁴²⁸ Hearing of Dec. 11, 2007, at 22 (transcript) (statement of Steven Engel).

⁴²⁹ Hearing of Dec. 11, 2007, at 22 (transcript) (statement of Steven Engel).

⁴³⁰ Hearing of Dec. 11, 2007, at 22 (transcript) (statement of Steven Engel).

⁴³¹ Hearing of Dec. 11, 2007, at 23 (transcript) (statement of Steven Engel).

⁴³² Hearing of Dec. 11, 2007, at 23 (transcript) (statement of Steven Engel).

Conclusion

This hearing investigated whether holding alien enemy combatants at Guantanamo Bay is in the best interests of our country, and to what legal rights the detainees were entitled. There was sharp division between the committee members. Those who supported keeping enemy combatants at Guantanamo noted that over 30 released former detainees had returned to wage war against America and its allies, while those opposed questioned these numbers and argued that the continued detention of prisoners was damaging U.S. standing abroad and had created a separate and unequal system of justice under U.S. law.

There was also sharp division within the Subcommittee regarding habeas corpus rights. Those who supported habeas rights for alien enemy combatants argued that it was dangerous to allow the President to hold such combatants indefinitely without ever charging them, noting that this war may not have a definitive end date. Opponents of extending habeas rights to detainees argued that habeas corpus rights have never been conferred upon prisoners of war, and that the Military Commissions Act and the Detainee Treatment Act provided detainees with unprecedented rights and a “day in court.” Ultimately, in June 2008, the United States Supreme Court held that federal habeas corpus rights extended to detainees held at Guantanamo, and that the Military Commissions Act of 2006 was an unconstitutional deprivation of that fundamental right.

Appendix: Hearings During the 110th Congress

**UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY**

US-VISIT: Challenges and Strategies for Securing the U.S. Border

31 January 2007

WITNESSES:

PANEL 1:

Richard Barth
Assistant Secretary
Office of Policy Development
Department of Homeland Security

Robert A. Mocny
Acting Director
US-VISIT Program
Department of Homeland Security

PANEL 2:

Richard Stana
Director
Homeland Security and Justice
Government Accountability Office

Phillip J. Bond
President and Chief Executive Officer
Information Technology Association

C. Stewart Verdery, Jr.
President
Monument Policy Group

Identity Theft: Innovative Solutions for an Evolving Problem

21 March 2007

WITNESSES:

PANEL 1:

Ronald Tenpas
Associate Deputy Attorney General
Department of Justice

Lydia Parnes
Director
Bureau of Consumer Protection
Federal Trade Commission

PANEL 2:

James Davis
Chief Information Officer
Vice Chancellor for Information Technology
University of California, Los Angeles

Joanne McNabb
Chief
California Office of Privacy Protection

Chris Jay Hoofnagle
Senior Staff Attorney
Samuelson Law, Technology, and Public Policy Clinic
University of California, Berkeley
School of Law

Interrupting Terrorist Travel: Strengthening the Security of International Travel
Documents

2 May 2007

WITNESSES:

PANEL 1:

Andrew Simkin
Director of Fraud Prevention Programs
Bureau of Consular Affairs
Department of State

Patrick Donovan
Assistant Director for Domestic Operations and
Acting Director of Diplomatic Security for Counter Measures
Diplomatic Security
Department of State

Michael P. Everitt
Unit Chief
Forensic Documents Laboratory
Immigration and Customs Enforcement
Department of Homeland Security

Paul Morris
Executive Director
Admissibility Requirements and Migration Control Office of Field Operations
US Customs and Border Protection

PANEL 2:

Ronald K. Noble
Secretary General of Interpol
Lyon, France

Clark Kent Ervin
Director of Homeland Security
Aspen Institute

Brian Zimmer
Senior Associate
Kelly, Anderson & Associates Inc.

The Legal Rights of Guantanamo Detainees: What Are They, Should They Be Changed,
and Is an End in Sight?

11 December 2007

WITNESSES:

PANEL 1:

Thomas Hartmann
Brigadier General
United States Air Force
Legal Advisor to the Convening Authority for Military Commissions

Steven Engel
Deputy Assistant Attorney General
Office of Legal Counsel, Department of Justice

PANEL 2:

Mark Denbeaux
Retired Seton Hall Law Professor

John Hutson
Rear Admiral
United States Navy
Dean, Franklin Pierce Law Center

Debra Burlingame
Member
Board of Directors of the National September 11 Memorial Foundation

Weaknesses in the Visa Waiver Program: Are the Needed Safeguards in Place to
Protect America?

28 February 2008

WITNESSES:

Stephen A. Edson
Deputy Assistant Secretary for Visa Services
Department of State

Jess T. Ford
Director
International Affairs and Trade
Government Accountability Office

Susan Ginsburg
Director
Mobility and Security Program
Migration Policy Institute

Paul Rosenzweig
Acting Assistant Secretary for International Affairs
Deputy Assistant Secretary for Policy
Department of Homeland Security

Jessica M. Vaughan
Policy Analyst
Center for Immigration Studies

The Visa Waiver Program: Mitigating Risks to Ensure Safety of All Americans

24 September 2008

WITNESSES:

Jess T. Ford
Director
International Affairs and Trade
Government Accountability Office

Stewart Baker
Assistant Secretary
Office of Policy
Department of Homeland Security